Schur rings over a product of Galois rings

Sergei Evdokimov
Steklov Institute of Mathematics
at St. Petersburg
evdokim@pdmi.ras.ru [*]

Ilia Ponomarenko
Steklov Institute of Mathematics
at St. Petersburg
inp@pdmi.ras.ru [†]

Abstract

The recently developed theory of Schur rings over a finite cyclic group is generalized to Schur rings over a ring R being a product of Galois rings of coprime characteristics. It is proved that if the characteristic of R is odd, then as in the cyclic group case any pure Schur ring over R is the tensor product of a pure cyclotomic ring and Schur rings of rank 2 over non-fields. Moreover, it is shown that in contrast to the cyclic group case there are non-pure Schur rings over R that are not generalized wreath products.

1 Introduction

In papers [12, 13] K. H. Leung and S. H. Man proved that any Schur ring (S-ring) over a finite cyclic group can be constructed from special S-rings by means of two operations: tensor product and wedge product (as for a background of S-rings see Section 2). This theorem supplemented with the normality theory from [4] enabled to get a series of strong results in algebraic combinatorics [4, 5, 11, 16].

To generalize the Leung-Man theorem in some way to S-rings over an arbitrary abelian group, the notion of S-ring over a commutative ring R[1] was

[*] The work was partially supported by RFFI Grant 07-01-00485.

[†] The work was partially supported by RFFI Grants 07-01-00485, 08-01-00379 and 08-01-00640.

[1] If the opposite is not indicated, all rings are supposed to be finite rings with identity.

introduced in [6]; by definition any such ring is an S-ring over the additive group R^+ of the ring R that is invariant with respect to its multiplicative group $R^\times$. It should be noted that by the Schur theorem on multipliers any S-ring over a cyclic group of order n can be treated as an S-ring over the ring $R = \mathbb{Z}_n$ of integers modulo n. We observe that in this case R is the direct product of Galois rings of coprime characteristics with prime residue fields. Thus it is natural to try to generalize the Leung-Man theorem to S-rings over the products of arbitrary Galois rings of coprime characteristics. In this paper such rings are called *CG-rings*.

The first step to constructing the theory of S-rings over rings is to characterize all primitive S-rings over a ring, i.e. those that have no proper quotients. The situation is controlled by a generalization of the Burnside-Schur theorem proved in [6] (see also Theorem 5.2). It turned out that any primitive S-ring over a ring R from a quite general class including all CG-rings is either of rank 2, or a cyclotomic ring over R (in the latter case R is a field). It should be mentioned that the special S-rings in the Leung-Man theorem belong exactly to one of these two classes. In [8] the Burnside-Schur theorem was applied to find a complete generalization of the Leung-Man theorem to S-rings over a Galois ring of odd characteristic.

On the second step, following the logic of the cyclic group case we should find a condition for an S-ring over a CG-ring R to be the generalized wreath product of S-rings over smaller CG-rings. (In the cyclic group case this operation was introduced in [3] and produces exactly the S-rings which are wedge products mentioned above.) In the case when R is a Galois ring of odd characteristic as well as in the cyclic case the required condition reduces to the non-purity of the S-ring in question. The latter means that any of its basic sets intersecting $R^\times$ is a union of cosets modulo a fixed non-zero ideal of R (see Subsection 5.2). However, the following theorem which we prove in Section 10 shows that the case of an arbitrary CG-ring is more complicated.

Theorem 1.1 *Let p and q be distinct primes, and d and e positive integers such that p divides $q^e - 1$ and q divides $p^d - 1$. Set $R = R_p \times R_q$ where $R_p = \mathrm{GR}(p^2, d)$ and $R_q = \mathrm{GR}(q^2, e)$. Then there exists a non-pure dense[2] S-ring over the CG-ring R that is not a non-trivial generalized wreath product.*

The S-rings from Theorem 1.1 never exist when $R = \mathbb{Z}_n$ because in this case $e = d = 1$ and the hypothesis is obviously not satisfied. It should be also

[2] As for the definition of density see the beginning of Section 8.

mentioned that probably all these S-rings are not schurian (as to the concept of schurity we refer to [9]). For example, this is the case when $(p, d) = (2, 2)$ and $(q, e) = (3, 1)$.

In spite of the fact that a complete analog for the non-pure part of the cyclic case theory can not be reconstructed for general CG-rings (Theorem 1.1), some information on non-pure S-rings over a CG-ring can be obtained. Namely, Theorem 7.1 in particular shows that any such ring which is not a non-trivial tensor or generalized wreath product, must "contain" all maximal and minimal ideals of R. (This theorem is also used to prove the density of pure S-rings.) The proof of this result occupies Sections 6 and 7. As an immediate consequence of Theorem 6.1 proved there we obtain the following classification of rational S-rings over a CG-ring, i.e. those any basic set of which is $R^\times$-invariant.

Theorem 1.2 *Any rational S-ring over a CG-ring is either a non-trivial generalized wreath product, or a tensor product, one factor of which is an S-ring of rank* 2.

At the final step we have to characterize pure S-rings over a CG-ring R. Again as in the cyclic group case we could expect that any such ring is the tensor product of a pure cyclotomic ring and S-rings of rank 2. However, this is not generally true. For example, if the characteristic of R is even, then there exist pure dense S-rings which are not cyclotomic. [3] The following statement shows that this obstacle is a unique one.

Theorem 1.3 *Any pure S-ring over a CG-ring of odd characteristic is the tensor product of a pure cyclotomic ring and S-rings of rank* 2 *over non-fields.*

Theorem 1.3 is an immediate consequence of Theorems 8.1 and 9.1 proved in Sections 8 and 9 respectively. In the proofs of these theorems we use the duality theory for S-rings over a CG-ring developed in Subsections 3.2 and 5.3. In the first case (Theorem 8.1) this theory shows that the property of an S-ring to be a non-trivial generalized wreath or tensor product is preserved under duality, and enables us to interchange minimal and maximal ideals of the ring. This reduces the proof to the dense case. In the second case (Theorem 9.1) we use another fact from this theory: an S-ring and its dual

[3] Some examples of such S-rings were found by the authors and will be published elsewhere.

are cyclotomic or not simultaneously. This enables us to prove that any dense pure S-ring over a CG-ring contains a pure cyclotomic S-ring. The rest of the proof is heavily based on Theorem 4.2 which applies to separate special pure sets by means of characters of the additive group of the underlying ring.

It should be stressed that this work was essentially influenced by papers [12] and [15]. However, there is a great difference between the cyclic group case and the general CG-ring case. Namely, in the former case the projection of any pure subgroup of the multiplicative group of the ring on at least one local component is also pure. On the contrary, in the latter one this is not true, e.g. for the CG-rings satisfying the hypothesis of Theorem 1.1. In fact, this is the only reason why the non-pure part of the theory can not be done properly. On the other hand, it is quite surprising that the pure part is completed by Theorem 1.2.

Concerning finite rings and permutation groups we refer to [14] and [2]. For the reader convenience we collect the basic facts on S-rings over abelian groups, on CG-rings and on S-rings over them in Sections 2, 3 and 5 respectively. In Section 4 we study pure sets in CG-rings. One of the main results here is the separation theorem (Theorem 4.2); the proof of it is given in Section 11.

Notation. As usual by $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ we denote the ring of integers, the ring of rationals and the field of complex numbers respectively.

For a prime p the pth part of a positive integer n is denoted by n_p.

For a commutative ring R with identity we denote by $R^\times$ and $\mathrm{rad}(R)$ the multiplicative group of R and the radical of R respectively.

The set of all (resp. all maximal, all minimal) ideals of R is denoted by $\mathcal{I}(R)$ (resp. $\mathcal{I}_{max}(R)$, $\mathcal{I}_{min}(R)$).

Given $I \in \mathcal{I}(R)$ we denote by I^+ the additive group of I, and by π_I the natural epimorphism from R to R/I.

For a set $X \subset R$ we denote by $I_{\mathrm{U}}(X)$ the smallest ideal of R containing X and by $I_{\mathrm{L}}(X)$ the largest ideal I of R such that $X + I = X$ or, equivalently, that X is a union of I-cosets. Also we set

$$\mathrm{ann}(X) = \{r \in R :\ rX = \{0\}\}$$

and write $\mathrm{ann}(r)$ instead of $\mathrm{ann}(\{r\})$ for $r \in R$.

Let $G = \prod_{p \in \mathcal{P}} G_p$ be a finite abelian group where $\mathcal{P} = \mathcal{P}(G)$ is the set of all primes dividing $|G|$ and G_p is the Sylow p-subgroup of G. For $Q \subset \mathcal{P}$

the Q-projection of $x \in G$ (resp. $X \subset G$) is denoted by x_Q (resp. X_Q). When $Q = \{p\}$ we omit the braces and we write Q' instead of $\mathcal{P} \setminus Q$. For an arbitrary set Q of primes we put $x_Q = x_{Q \cap \mathcal{P}}$ and $X_Q = X_{Q \cap \mathcal{P}}$.

For a subset X of a group G we set $X^{\#} = X \setminus \{1_G\}$.

The group ring of a group G over an arbitrary ring R is denoted by RG. The element of RG that is equal to the sum of all elements of a set $X \subset G$ is denoted by $\xi(X)$. The support of $\xi \in RG$ is denoted by $\mathrm{Supp}(\xi)$. The componentwise multiplication in RG is denoted by $\circ$.

2 S-rings over groups

2.1 Definition and properties. Let G be a finite group. A subring $\mathcal{A}$ of the group ring $\mathbb{Z}G$ is called a *Schur ring* (*S-ring*, for short) over G if it has a (uniquely determined) $\mathbb{Z}$-basis consisting of the elements $\xi(X) = \sum_{x \in X} x$ where X runs over a family $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of pairwise disjoint non-empty subsets of G such that

$$\{1\} \in \mathcal{S}, \quad \bigcup_{X \in \mathcal{S}} X = G \quad \text{and} \quad X \in \mathcal{S} \ \Rightarrow \ X^{-1} \in \mathcal{S}.$$

We call the elements of $\mathcal{S}$ the *basic* sets of $\mathcal{A}$ and denote by $\mathcal{S}^*(\mathcal{A})$ the set of all unions of them and by $\mathcal{H}(\mathcal{A})$ the set of all subgroups of G in $\mathcal{S}^*(\mathcal{A})$. The elements of $\mathcal{S}^*(\mathcal{A})$ and $\mathcal{H}(\mathcal{A})$ are called *$\mathcal{A}$-subsets of G* (or *$\mathcal{A}$-sets*) and *$\mathcal{A}$-subgroups of G* respectively. It is easily seen that XY is an $\mathcal{A}$-set whenever so are X and Y. For an $\mathcal{A}$-set X we put

$$\mathcal{S}_X = \{X' \in \mathcal{S} : \ X' \subset X\}.$$

The number $\mathrm{rk}(\mathcal{A}) = \dim_{\mathbb{Z}}(\mathcal{A})$ is called the *rank* of $\mathcal{A}$. If $\mathcal{S}^*(\mathcal{A}) \subset \mathcal{S}^*(\mathcal{A}')$ where $\mathcal{A}'$ is an S-ring over G, then we write $\mathcal{A} \le \mathcal{A}'$.

Lemma 2.1 *Let $\mathcal{A}$ be an S-ring over a group G, $H \in \mathcal{H}(\mathcal{A})$ and $X \in \mathcal{S}(\mathcal{A})$. Then the cardinality of the set $X_{H,x} = X \cap Hx$ does not depend on $x \in X$.*

Proof. See [8, p.21].■

Let $H \in \mathcal{H}(\mathcal{A})$. Then $\mathcal{S}_H$ where $\mathcal{S} = \mathcal{S}(\mathcal{A})$, is the set of basic sets of an S-ring over the group H. This S-ring is denoted by $\mathcal{A}_H$. If the group H is normal and $\pi : G \to G/H$ is the quotient epimorphism, then $\mathcal{S}_{G/H} = \pi(\mathcal{S})$ is the set of basic sets of an S-ring over the group G/H. This S-ring is denoted by $\mathcal{A}_{G/H}$.

If $\mathcal{A}_1$ and $\mathcal{A}_2$ are S-rings over groups G_1 and G_2 respectively, then the subring $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ of the ring $\mathbb{Z}G_1 \otimes \mathbb{Z}G_2 = \mathbb{Z}G$ where $G = G_1 \times G_2$, is an S-ring over the group G with

$$\mathcal{S}(\mathcal{A}) = \{X_1 \times X_2 : X_1 \in \mathcal{S}(\mathcal{A}_1),\ X_2 \in \mathcal{S}(\mathcal{A}_2)\}.$$

It is called the *tensor product* of $\mathcal{A}_1$ and $\mathcal{A}_2$.

Lemma 2.2 *Let G_1 and G_2 be groups, and $\mathcal{A}$ an S-ring over the group $G = G_1 \times G_2$. Suppose that $G_1, G_2 \in \mathcal{H}(\mathcal{A})$. Then $\pi_i(X) \in \mathcal{S}(\mathcal{A})$ for all $X \in \mathcal{S}(\mathcal{A})$ where π_i is the projection of G on G_i, $i = 1, 2$. In particular, $\mathcal{A} \ge \mathcal{A}_{G_1} \otimes \mathcal{A}_{G_2}$.*

Proof. Let $X \in \mathcal{S}(\mathcal{A})$ and $i \in \{1, 2\}$. Then obviously $G_{3-i}X \cap G_i = \pi_i(X)$. By the hypothesis this implies that $\pi_i(X) \in \mathcal{S}^*(\mathcal{A})$. To complete the proof it suffices to note that if $\pi_i(X)$ is the disjoint union of non-empty $\mathcal{A}$-sets Y and Z, then X is the disjoint union of the non-empty $\mathcal{A}$-sets $X \cap G_{3-i}Y$ and $X \cap G_{3-i}Z$ which is impossible because $X \in \mathcal{S}(\mathcal{A})$.■

Let $\mathcal{A}$ be an S-ring over a group G and let L, U be $\mathcal{A}$-subgroups of G such that $L \le U$ and L is normal in G. Following [4] we say that $\mathcal{A}$ satisfies the *U/L-condition* if

$$LX = XL = X, \qquad X \in \mathcal{S}(\mathcal{A})_{G \setminus U}.$$

If, moreover, $L \ne \{1\}$ and $U \ne G$, we say that $\mathcal{A}$ satisfies the U/L-condition *non-trivially.*

An S-ring $\mathcal{A}$ satisfying the U/L-condition was called in [12, 13] the wedge product of the S-rings $\mathcal{A}_U$ and $\mathcal{A}_{G/L}$. It should be noted that the authors in [3] independently introduced the external operation of the generalized wreath product of two S-rings which produces exactly the S-rings satisfying the U/L-condition.

The following important theorem goes back to I. Schur and H. Wielandt (see [17, Ch. IV]); as to the formulation given here we refer to [6]. Below for $X \subset G$, $m \in \mathbb{Z}$, and a prime p we set

$$X^{(m)} = \{x^m :\ x \in X\}, \quad X^{[p]} = \{x^p :\ x \in X,\ |xH \cap X| \not\equiv 0 \pmod p\}$$

where $H = \{g \in G :\ g^p = 1\}$.

Theorem 2.3 *Let G be a finite abelian group and $\mathcal{A}$ an S-ring over G. Then for any $X \in \mathcal{S}(\mathcal{A})$ the following statements hold:*

(1) $X^{(m)} \in \mathcal{S}(\mathcal{A})$ *for any integer m coprime to $|G|$,*

(2) $X^{[p]} \in \mathcal{S}^*(\mathcal{A})$ *for any prime p dividing $|G|$.*$\blacksquare$

2.2 Duality. Let $\mathcal{A}$ be an S-ring over a finite abelian group G and $\widehat{G}$ the group dual to G, i.e. the group of all irreducible $\mathbb{C}$-characters of G. Given $S \subset G$ and $\chi \in \widehat{G}$ set

$$\chi(S) = \sum_{s \in S} \chi(s). \tag{1}$$

Characters $\chi_1, \chi_2 \in \widehat{G}$ are called equivalent if $\chi_1(S) = \chi_2(S)$ for all $S \in \mathcal{S}(\mathcal{A})$. Denote by $\widehat{\mathcal{S}}$ the set of classes of this equivalence relation. Then the submodule of $\mathbb{Z}\widehat{G}$ spanned by the elements $\xi(X)$, $X \in \widehat{\mathcal{S}}$, is an S-ring over $\widehat{G}$ (see [1, Theorem 6.3]). This ring is called *dual* to $\mathcal{A}$ and is denoted by $\widehat{\mathcal{A}}$. Obviously, $\mathcal{S}(\widehat{\mathcal{A}}) = \widehat{\mathcal{S}}$. Moreover, $\mathrm{rk}(\widehat{\mathcal{A}}) = \mathrm{rk}(\mathcal{A})$ and

$$\mathcal{H}(\widehat{\mathcal{A}}) = \{H^\perp : \ H \in \mathcal{H}(\mathcal{A})\} \tag{2}$$

where $H^\perp = \{\chi \in \widehat{G} : \ H \leq \ker(\chi)\}$. It is also true that the S-ring dual to $\widehat{\mathcal{A}}$ is equal to $\mathcal{A}$. The following theorem was proved in [8].

Theorem 2.4 *Let $\mathcal{A}$ be an S-ring over an abelian group G. Then $\mathcal{A}$ satisfies the U/L-condition if and only if $\widehat{\mathcal{A}}$ satisfies the $L^\perp/U^\perp$-condition.*$\blacksquare$

Some more properties of the dual S-ring are contained in the following statement.

Theorem 2.5 *Let $\mathcal{A}$ be an S-ring over an abelian group G. Then*

(1) $\widehat{\mathcal{A}_H} = \widehat{\mathcal{A}}_{\widehat{G}/H^\perp}$ *and* $\widehat{\mathcal{A}_{G/H}} = \widehat{\mathcal{A}}_{H^\perp}$ *for any $H \in \mathcal{H}(\mathcal{A})$,*

(2) $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ *if and only if* $\widehat{\mathcal{A}} = \widehat{\mathcal{A}}_1 \otimes \widehat{\mathcal{A}}_2$.

Proof. To prove statement (1) it suffices to verify the second equality. It is easily seen that $\chi(X) = a\chi(XH)$ for all $\chi \in H^\perp$ and $X \in \mathcal{S}(\mathcal{A})$ where a is a positive rational. So for any $\chi_1, \chi_2 \in H^\perp$ we have

$$\chi_1(XH) = \chi_2(XH) \ \Leftrightarrow \ \chi_1(X) = \chi_2(X)$$

and we are done by the definition of the dual S-ring. To prove statement (2) suppose that $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$. Then $G = G_1 \times G_2$ where $G_1, G_2 \in \mathcal{H}(\mathcal{A})$, and $\mathcal{A}_1 = \mathcal{A}_{G_1} = \mathcal{A}_{G/G_2}$ and $\mathcal{A}_2 = \mathcal{A}_{G_2} = \mathcal{A}_{G/G_1}$ (see Lemma 2.2). Therefore from statement (1) it follows that

$$\widehat{\mathcal{A}}_i = \widehat{\mathcal{A}_{G_i}} = \widehat{\mathcal{A}_{G/G_{3-i}}} = \widehat{\mathcal{A}}_{G_{3-i}^{\perp}}, \qquad i = 1, 2$$

(we identify $\widehat{G_i}$ and $G_{3-i}^{\perp}$). Since obviously $\widehat{G} = G_1^{\perp} \times G_2^{\perp}$ and $G_1^{\perp}, G_2^{\perp} \in \mathcal{H}(\widehat{\mathcal{A}})$ (see (2)), this implies that $\widehat{\mathcal{A}} \geq \widehat{\mathcal{A}}_1 \otimes \widehat{\mathcal{A}}_2$. Since also $\mathrm{rk}(\widehat{\mathcal{A}_i}) = \mathrm{rk}(\mathcal{A}_i)$, $i = 1, 2$, and $\mathrm{rk}(\mathcal{A}) = \mathrm{rk}(\widehat{\mathcal{A}})$, we conclude that $\widehat{\mathcal{A}} = \widehat{\mathcal{A}}_1 \otimes \widehat{\mathcal{A}}_2$.■

3 CG-rings

Throughout the rest of the paper under a ring we mean a finite commutative ring with identity.

3.1 Products of Galois rings. Following [14, Section XVI] a local ring R is called *Galois* if it is a Galois extension of the prime ring $\mathbb{Z}_{p^n}$ for some prime p and positive integer n, or equivalently if $\mathrm{rad}(R) = pR$. Given positive integers n, d there exists a unique (up to isomorphism) Galois ring of characteristic p^n with the residue field of order $q = p^d$; it is denoted by $\mathrm{GR}(p^n, d)$. We observe that

$$\mathrm{GR}(p, d) \cong \mathrm{GF}(p^d), \qquad \mathrm{GR}(p^n, 1) \cong \mathbb{Z}_{p^n}.$$

Each ideal of the Galois ring $\mathrm{GR}(p^n, d) = R$ other than R is of the form $p^i R$, $i = 1, \ldots, n$, and the corresponding quotient ring is isomorphic to $\mathrm{GR}(p^i, d)$. It is known that R^+ is a homocyclic p-group of rank d and exponent p^n, i.e. it is isomorphic to the direct product of d cyclic groups of order p^n. Moreover,

$$R^{\times} = \mathcal{T} \times \mathcal{U} \tag{3}$$

where $\mathcal{T}$ is the Teichmüller group and $\mathcal{U}$ is the group of principal units. The groups $\mathcal{T}$ and $\mathcal{U} = 1 + \mathrm{rad}(R)$ are a cyclic group of order $q-1$ and an abelian p-group respectively. If p is odd, then the group $\mathcal{U}$ is homocyclic of rank d and exponent p^{n-1}.

Let R be a ring and $\mathcal{P} = \mathcal{P}(R)$. It is well known (see e.g. [14, Theorem 6.2]) that there is a decomposition

$$R = \prod_{p \in \mathcal{P}} R_p$$

where R_p is the *p-component* of R, i.e. the subring of R such that $(R_p)^+$ is the Sylow p-subgroup of R^+. Moreover, each R_p is the direct product of local rings the characteristic of each of which is a power of p. For any $Q \subset \mathcal{P}$ the set R_Q (defined in Notation) equals the product of all rings R_p with $p \in Q$.

Definition 3.1 *We say that R is a CG-ring (componentwise Galois ring) if R_p is a Galois ring for all $p \in \mathcal{P}$.*

Obviously, the ring with one element as well as any Galois ring is CG. The characteristic c of a CG-ring R equals the product of the characteristics c_p of its components R_p, $p \in \mathcal{P}$. It is easily seen that

$$\mathcal{I}(R) = \{mR : \ m \text{ divides } c\}. \tag{4}$$

In particular, the minimal and maximal ideals of R are exactly those mR for which respectively $m = c/p$ and $m = p$ where $p \in \mathcal{P}$. Throughout the paper we denote by I_0 the sum of minimal ideals in the components and set $I_{0,p} = (I_0)_p$. Clearly,

$$I_{0,p} = (c_p/p)R_p, \qquad p \in \mathcal{P}. \tag{5}$$

One can see that given $I \in \mathcal{I}(R)$ the set $1 + I$ is a subgroup of $R^\times$ if and only if $I_p \neq R_p$ for all $p \in \mathcal{P}(I)$.

The class of all CG-rings is closed with respect to taking quotients. Moreover, the following equality holds:

$$\pi_I(R)^\times = \pi_I(R^\times), \qquad I \in \mathcal{I}(R). \tag{6}$$

Let $a \in R$. Then the mapping $x \mapsto ax$, $x \in R$, induces an R-module epimorphism from R onto $I = aR$ the kernel of which coincides with $\operatorname{ann}(a)$. Therefore the ring $R/\operatorname{ann}(a)$ and the ideal I are isomorphic as R-modules. This enables us to define a ring structure on the ideal I. The corresponding ring $R_{I,a}$ has a as identity and

$$f_{I,a} : R \to R_{I,a}, \quad x \mapsto ax \tag{7}$$

is a ring epimorphism with the kernel $\operatorname{ann}(a)$. It should be noted that for any $u \in R^\times$ the rings $R_{I,a}$ and $R_{I,ua}$ are isomorphic. When $a = m \cdot 1$ where

m is a positive integer dividing the characteristic of R, we set $R_I = R_{I,a}$ and $f_I = f_{I,a}$. From (4), (6) and (7) it follows that in this case

$$(R_I)^\times = mR^\times. \tag{8}$$

In this paper we consider the permutation group induced by the action of the group $R^\times$ on the set R by multiplication. It is a subgroup of the group $\mathrm{Aut}(R^+)$ that leaves any ideal of R fixed. Moreover, the orbits of this group are regular and $R^\times$ is the only faithful one.

3.2 Duality. Let R be a CG-ring of characteristic c and $\mathcal{P} = \mathcal{P}(R)$. For each $p \in \mathcal{P}$ denote by χ_p a character of the group $(R_p)^+$ such that $\mathrm{im}(\chi_p)$ contains a primitive c_pth root of unity, and by $\widehat{R}_p$ the Galois ring *dual* to R_p with respect to χ_p (see [8]). The CG-ring

$$\widehat{R} = \prod_{p\in\mathcal{P}} \widehat{R}_p$$

is called *dual* to R with respect to the character $\chi = \prod_p \chi_p$. Clearly, $\widehat{R}^+ = \widehat{R^+}$ is the group dual to the group R^+, and

$$(mR)^\perp = (c/m)\widehat{R} \tag{9}$$

where m is a divisor of c. Moreover, $\widehat{R} = \{\chi^{(r)} :\ r \in R\}$ where $\chi^{(r)}$ is the character of R^+ such that $\chi^{(r)}(x) = \chi(rx)$, $x \in R$, and the multiplication in $\widehat{R}$ is defined by the formula $\chi^{(r)}\chi^{(s)} = \chi^{(rs)}$, $r, s \in R$. Thus χ is the identity of this ring and

$$\widehat{R}^\times = \{\chi^{(r)} :\ r \in R^\times\}. \tag{10}$$

The mapping $r \mapsto \chi^{(r)}$ is a ring isomorphism from R onto $\widehat{R}$; the image of a group $K \le R^\times$ with respect to this isomorphism is denoted by $\widehat{K}$.

4 Purity in CG-rings

Let R be a ring. Following [7] a non-empty set $X \subset R$ is called *pure* if $I_{\mathrm{L}}(X) = 0$. This means that given $I \in \mathcal{I}(R)$ the equality $X + I = X$ implies $I = 0$. Thus a non-empty set is non-pure if and only if it is a union of I-cosets for some non-zero ideal I. It is clear that

$$I_{\mathrm{L}}(X) = I_{\mathrm{L}}(uX), \quad u \in R^\times, \tag{11}$$

and hence the sets X and uX are pure or not simultaneously. Therefore any subset of a pure orbit of a subgroup of $R^\times$ is also pure. It should be also noted that the purity of a group $K \le R^\times$, is equivalent to the fact that K does not contain any subgroup of the form $1 + I$ where I is a non-zero ideal of R.

We note that generally the purity of a set is not preserved under taking quotients or multiplying by integer. For instance, let

$$R = \mathbb{Z}_8, \quad X = \{-1, 1\}, \quad I = 4R.$$

Then the set X is pure whereas the sets $\pi_I(X)$, $2X$ are not. However, for CG-rings of odd characteristic the situation is controlled as follows.

Theorem 4.1 *Let R be a CG-ring of odd characteristic, $K \le R^\times$ a pure group and J an ideal of R. Suppose that $J_p \ne R_p$ for all $p \in \mathcal{P}$. Then the group $\pi_J(K)$ and the set $c_J K$ are pure where c_J is the characteristic of J.*

Proof. Since the ring R/J and the ideal $c_J R$ are isomorphic as R-modules, it suffices to verify only that the set $\pi_J(K)$ is pure. To do this we start with two observations. First, the condition $J_p \ne R_p$ for all $p \in \mathcal{P}$, implies that the set $1 + J$ is a subgroup of the group $R^\times$. Therefore there is a canonical isomorphism

$$\pi_J(L) \cong L/(L \cap (1 + J)), \qquad L \le R^\times. \tag{12}$$

Second, denote by r_p the degree of the residue field of the ring R_p over the prime subfield, $p \in \mathcal{P}$. Then $r_p = \mathrm{rk}(\mathcal{U}_p)$ whenever R_p is not a field where $\mathcal{U}_p$ is the group of principal units of the ring R_p. We claim that for any $L \le R^\times$ the following equivalence holds

$$L \text{ is pure} \quad \Leftrightarrow \quad \mathrm{rk}(L \cap \mathcal{U}_p) < r_p \text{ for all } p \in \mathcal{P}. \tag{13}$$

To prove (13) we observe that since L is a group, given an ideal $I \in \mathcal{I}(R)$ we have $L = L + I$ if and only if $L \ge 1 + I$. Therefore the group L is non-pure if and only if $L \ge 1 + I$ for some non-zero ideal I of R (here $0 \ne I_p \ne R_p$ for all $p \in \mathcal{P}(I)$). The latter is equivalent to the existence of $p \in \mathcal{P}$ such that $L \ge 1 + I_{0,p}$ (here $I_{0,p} \ne R_p$, see above). However, this means that

$$\mathrm{rk}(1 + I_{0,p}) = \mathrm{rk}(\mathcal{U}_p) = r_p \quad \text{and} \quad L \cap \mathcal{U}_p \ge 1 + I_{0,p},$$

i.e. $\mathrm{rk}(L \cap \mathcal{U}_p) \ge \mathrm{rk}(1 + I_{0,p}) = r_p$.

To complete the proof we note that the rank of an abelian group does not increase under taking quotients. Therefore from (12) we obtain

$$\mathrm{rk}(\pi_J(K)\cap\pi_J(\mathcal{U}_p)) = \mathrm{rk}((K\cap\mathcal{U}_p)/(K\cap\mathcal{U}_p\cap(1+J)) \le \mathrm{rk}(K\cap\mathcal{U}_p) < r_p$$

for all $p\in\mathcal{P}$. Since the degree of the residue field of the ring $\pi_J(R_p)$ equals r_p and the group of principal units of the latter ring coincides with $\pi_J(\mathcal{U}_p)$, we are done by (13).■

The following important statement which will be used in Section 9 is a kind of separation theorem for pure subsets in CG-rings of an arbitrary characteristic.

Theorem 4.2 *Let R be a CG-ring, and $S, S'\subset R$ distinct subsets in a pure orbit of a subgroup of $R^\times$, $S\ne\emptyset$. Then*

(1) *there exists $\chi\in\widehat{R}^\times$ such that $\chi(S)\ne\chi(S')$,*

(2) *given $\chi\in\widehat{R}^\times$ there exists $r\in R^\times$ such that $\chi(rS)\ne 0$.*

The proof of this theorem is given in Section 11.

5 S-rings over a CG-ring

5.1 Definition and properties. Let R be a ring and $\mathcal{A}$ an S-ring over the group R^+. In accordance with [6] we say that $\mathcal{A}$ is an *S-ring over R* if it is invariant with respect to the action of the group $R^\times$ on $\mathbb{Z}R^+$ by multiplication, or, equivalently, if for any $u\in R^\times$

$$X\in\mathcal{S}(\mathcal{A})\quad\Rightarrow\quad uX\in\mathcal{S}(\mathcal{A}). \tag{14}$$

One can see that this is the case if $\mathrm{rk}(\mathcal{A})=2$ or $\mathcal{S}(\mathcal{A})=\mathrm{Orb}(K,R)$ for some $K\le R^\times$. In the latter case $\mathcal{A}$ is called *cyclotomic* and denoted by $\mathrm{Cyc}(K,R)$. Clearly,

$$\mathrm{Cyc}(K,R)=\mathrm{span}\{\xi(X):\ X\in\mathrm{Orb}(K,R)\}.$$

Since the group K acts semiregularly on $R^\times$, the cyclotomic rings are in 1-1 correspondence to the subgroups of $R^\times$. The following result is a special case of [8, Corollary 2.3].

Theorem 5.1 *Let $\mathcal{A}$ be an S-ring over a ring R. Then any basic set of $\mathcal{A}$ contained in $R^\times$ is a subgroup of $R^\times$. In particular, any S-ring over a field is a cyclotomic one.*$\blacksquare$

Let $\mathcal{A}$ be an S-ring over the ring R. Set

$$\mathcal{I}(\mathcal{A}) = \mathcal{I}(R, \mathcal{A}) = \{I \in \mathcal{I}(R) : \; I \in \mathcal{S}^*(\mathcal{A})\}.$$

The elements of $\mathcal{I}(\mathcal{A})$ are called $\mathcal{A}$-*ideals* of R. It was proved in [8, Theorem 2.6] that if a ring R is generated by the units, then

$$I_{\mathrm{U}}(X), I_{\mathrm{L}}(X) \in \mathcal{I}(\mathcal{A}), \qquad X \in \mathcal{S}^*(\mathcal{A}). \tag{15}$$

Since the assumption is true for every local ring, the conclusion holds when R is a CG-ring. From now on we assume that R is a CG-ring.

Let $\mathcal{A}$ be an S-ring over the ring R and $I \in \mathcal{I}(\mathcal{A})$. Since the ring $\mathcal{A}$ is $R^\times$-invariant, the S-rings $\mathcal{A}_{R/I} = \mathcal{A}_{R^+/I^+}$ and $\mathcal{A}_I = \mathcal{A}_{I^+}$ over the groups R^+/I^+ and I^+ are $(R/I)^\times$- and $(R_I)^\times$-invariant respectively. Thus they are S-rings over the rings R/I and R_I.

The S-ring $\mathcal{A}$ is called *dense* if $\mathcal{I}(\mathcal{A}) = \mathcal{I}(R)$. From (4) it follows that the set-difference between an ideal of R and the union of all proper ideals in it is an orbit of the group $R^\times$. Therefore

$$R^\times r \in \mathcal{S}^*(\mathcal{A}), \qquad r \in R. \tag{16}$$

We say that $\mathcal{A}$ is *R-primitive* if 0 and R are the only $\mathcal{A}$-ideals of R. The following theorem is a special case of the main result of [6].

Theorem 5.2 *Let R be a CG-ring. Then any R-primitive S-ring is either of rank* 2 *or cyclotomic.*[4] *In the latter case, R is a field.*$\blacksquare$

The following statement will be used in the proof of Theorem 6.3. (In fact, the proof shows that the conclusion is true under a weaker assumption that the p-component of the ring R is a Galois ring.)

Theorem 5.3 *Let R be a CG-ring of characteristic c and $\mathcal{A}$ an S-ring over R. Then for any $p \in \mathcal{P}(R)$ and $X \in \mathcal{S}(\mathcal{A})$ such that $R_p^\times X = X$, the following statements hold:*

[4] In the conditions of the theorem "R-primitivity" is equivalent to "quasiprimitivity" in sense of [6] (see the remark before Theorem 1.3 of that paper).

(1) $(X^{[p]})_p = \{0\}$,

(2) $I_{\mathrm{L}}(X)_p \ne 0$ *if and only if* $X^{[p]} = \emptyset$,

(3) *if* $I_{\mathrm{L}}(X)_p = 0$, *then either* $X_p = \{0\}$ *or* $I_{\mathrm{L}}(X \cup Y)_p \ne 0$ *with* $Y = (X^{[p]})^{(m)}$ *where* m *is an integer coprime to* c *such that* $mp \equiv 1 \,(\mathrm{mod}\, c_{p'})$.

Proof. Let $p \in \mathcal{P}(R)$ and $X \in \mathcal{S}(\mathcal{A})$ be such that $R_p^\times X = X$. Take $x \in X$. Then $R_p^\times x \subset X$. On the other hand, set $J = I_{0,p}$ (see (5)). Since R is a CG-ring, R_p is a Galois ring, and hence the set $x_p R_p^\times$ is either a J-coset, or $J^\#$, or $\{0\}$ (in the latter two cases the order of x_p is p and 1 respectively). Thus

$$X_{x,J} \ne x + J \quad \Leftrightarrow \quad X_{x,J} = x_{p'} + J^\# \text{ or } X_{x,J} = \{x_{p'}\}. \tag{17}$$

From the hypothesis of the theorem it follows that the set of all elements of order p in R coincides with $J^\#$. Since X is a union of all sets $X_{x,J}$, $x \in X$, we conclude by (17) and statement (2) of Theorem 2.3 that $X^{[p]} = pX'$ where X' is the set of all $x \in X$ for which the condition in the right-hand side of (17) holds (here we use this theorem for additively written group $G = R^+$; in this case $H = J$ and $xH \cap X = X_{J,x}$). This proves statement (2), and due to the obvious equality $(pX')_p = \{0\}$ also statement (1). To prove statement (3) suppose that $I_{\mathrm{L}}(X \cup Y)_p = 0$. Then since

$$Y = (X^{[p]})^{(m)} = (pX')^{(m)} = mpX' = (X')_{p'}, \tag{18}$$

from (17) it follows that there exists $x \in X'$ for which $X_{x,J} = \{x_{p'}\}$. However, in this case $x = x_{p'}$, and hence $x \in X \cap Y$. Taking into account that $X \in \mathcal{S}(\mathcal{A})$ and $Y \in \mathcal{S}^*(\mathcal{A})$ (Theorem 2.3), we conclude that $X \subset Y$. This implies by (18) that $X_p \subset Y_p = \{0\}$ which completes the proof.■

5.2 Pure S-rings and generalized wreath products. Let $\mathcal{A}$ be an S-ring over a CG-ring R. Due to (11) the ideal $I_{\mathrm{L}}(X)$ does not depend on the set $X \in \mathcal{S}(\mathcal{A})$ such that $X \cap R^\times \ne \emptyset$. We denote this ideal by $I_{\mathrm{L}}(\mathcal{A})$.

Definition 5.4 *The S-ring* $\mathcal{A}$ *is pure if* $I_{\mathrm{L}}(\mathcal{A}) = 0$.

It follows that $\mathcal{A}$ is pure if and only if some (and hence any) $X \in \mathcal{S}(\mathcal{A})$, $X \cap R^\times \ne \emptyset$, is pure. It is easily seen that S-rings of rank 2 and cyclotomic rings $\mathrm{Cyc}(K, R)$ with pure groups $K \le R^\times$, are pure.

Theorem 5.5 *Let R be a CG-ring of odd characteristic and $\mathcal{A}$ a pure S-ring over R. Suppose that $\mathcal{I}_{max}(R) \subset \mathcal{I}(\mathcal{A})$ and J is an $\mathcal{A}$-ideal of R such that $J_p \neq R_p$ for all $p \in \mathcal{P}(R)$. Then the S-ring $\mathcal{A}_{R/J}$ is also pure.*

Proof. Let $Y \in \mathcal{S}(\mathcal{A}_{R/J})$ be such that $\pi(1) \in Y$ where $\pi = \pi_J$. Then it suffices to verify that the set Y is pure. To do this denote by X the basic set of $\mathcal{A}$ containing 1. Then obviously $Y = \pi(X)$. Moreover, since by the hypothesis $\mathcal{I}_{max}(R) \subset \mathcal{I}(\mathcal{A})$, it follows that $R^\times$ is an $\mathcal{A}$-set, and hence $X \subset R^\times$. So X is a subgroup of $R^\times$ by Theorem 5.1. However, the set X is pure because so is the S-ring $\mathcal{A}$. Therefore the set $Y = \pi(X)$ is pure by Theorem 4.1 and we are done.■

In [8, Theorem 2.8] it was proved that an S-ring over a local ring is non-pure if and only if it is a non-trivial generalized wreath product. However, this is not true for the S-rings over an arbitrary CG-ring (see Section 10). Since most of the results in this paper are formulated in terms of that product, we recall its definition here.

Definition 5.6 *We say that $\mathcal{A}$ is a generalized wreath product if there exist $\mathcal{A}$-ideals I and J such that*

$$J \subset I_{\mathrm{L}}(X) \cap I, \qquad X \in \mathcal{S}(\mathcal{A})_{R \setminus I}. \tag{19}$$

In this case we also say that $\mathcal{A}$ satisfies the I/J-condition.

If both ideals I and J are proper, we say that the generalized wreath product is *non-trivial*, or that the S-ring $\mathcal{A}$ satisfies the I/J-condition *non-trivially.*

It should be noted that the S-ring $\mathcal{A}$ satisfying the I/J-condition satisfies also the I^+/J^+-condition as defined in Subsection 2.1. Therefore in the sense of [3] in this case the S-ring $\mathcal{A}$ is the (standard) generalized wreath product of the S-rings $\mathcal{A}_I$ and $\mathcal{A}_{R/J}$ over the groups I^+ and $(R/J)^+$ respectively. Moreover, the latter S-ring can be treated as an S-ring over the ring R/J whereas the former one can be treated as an S-ring over the ring R_I defined in Subsection 3.1.

5.3 Duality. Let $\widehat{R}$ be the ring dual to a CG-ring R with respect to a character χ. We observe that since the set $\widehat{R}^\times$ does not depend on the choice of χ, any S-ring over this ring is also an S-ring over the ring dual to R with respect to any other character belonging to $\widehat{R}^\times$.

Theorem 5.7 *Let $\mathcal{A}$ be an S-ring over a CG-ring R and $\widehat{\mathcal{A}}$ the S-ring over the group $\widehat{R}^+$ that is dual to $\mathcal{A}$. Then $\widehat{\mathcal{A}}$ is an S-ring over the ring $\widehat{R}$.*

Proof. Suppose that $\chi^{(s)}$ and $\chi^{(t)}$ belong to the same basic set of $\widehat{\mathcal{A}}$ where $s, t \in R$. Then given $r \in R^\times$ we have $\chi^{(s)}(rS) = \chi^{(t)}(rS)$, or equivalently

$$\chi^{(rs)}(S) = \chi^{(rt)}(S), \quad S \in \mathcal{S}(\mathcal{A}).$$

Since $\chi^{(rs)} = \chi^{(r)}\chi^{(s)}$ and $\chi^{(rt)} = \chi^{(r)}\chi^{(t)}$, this implies that the characters $\chi^{(r)}\chi^{(s)}$ and $\chi^{(r)}\chi^{(t)}$ belong to the same basic set of $\widehat{\mathcal{A}}$ for all $r \in R^\times$. Thus the required statement follows from (10).■

Let c be the characteristic of the ring R (and hence of the ring $\widehat{R}$). Then $\mathcal{I}(R) = \{mR : \ m \text{ divides } c\}$ and $\mathcal{I}(\widehat{R}) = \{m\widehat{R} : \ m \text{ divides } c\}$. Therefore by (9) and (2) we have

$$\mathcal{I}(\widehat{\mathcal{A}}) = \{I^\perp : \ I \in \mathcal{I}(\mathcal{A})\}. \tag{20}$$

Thus $\mathcal{A}$ is R-primitive if and only if $\widehat{\mathcal{A}}$ is $\widehat{R}$-primitive. Moreover, from (20) and Theorem 2.4 we obtain the following statement.

Theorem 5.8 *Let $\mathcal{A}$ be an S-ring over a CG-ring. Then the ring $\mathcal{A}$ is a non-trivial generalized wreath product if and only if so is the ring $\widehat{\mathcal{A}}$. More exactly, $\mathcal{A}$ satisfies the I/J-condition if and only if $\widehat{\mathcal{A}}$ satisfies the $J^\perp/I^\perp$-condition.*■

The following theorem shows that an S-ring and its dual are cyclotomic or not simultaneously. This fact can also be deduced from the results of [10] by using the well-known 1-1 correspondence between S-rings and translation association schemes.

Theorem 5.9 *Let $\mathcal{A} = \mathrm{Cyc}(K, R)$ where $K \le R^\times$. Then $\widehat{\mathcal{A}} = \mathrm{Cyc}(\widehat{K}, \widehat{R})$.*

Proof. Let $X \in \mathrm{Orb}(\widehat{K}, \widehat{R})$. Then given $\chi_1, \chi_2 \in X$ there exists $r \in K$ such that $\chi_1 = \chi_2^{(r)}$. Since $S = rS$ for each basic set S of $\mathcal{A}$, this implies that

$$\chi_1(S) = \chi_2^{(r)}(S) = \chi_2(rS) = \chi_2(S), \qquad S \in \mathcal{S}(\mathcal{A}).$$

Therefore $\mathcal{A}' \ge \widehat{\mathcal{A}}$ where $\mathcal{A}' = \mathrm{Cyc}(\widehat{K}, \widehat{R})$. On the other hand, $\mathrm{rk}(\widehat{\mathcal{A}}) = \mathrm{rk}(\mathcal{A})$ (see Subsection 2.2). Moreover, since there is a ring isomorphism from R to $\widehat{R}$ taking K to $\widehat{K}$ (see Subsection 3.2), we also have $\mathrm{rk}(\mathcal{A}) = \mathrm{rk}(\mathcal{A}')$. Thus $\mathrm{rk}(\widehat{\mathcal{A}}) = \mathrm{rk}(\mathcal{A}')$ whence it follows that $\widehat{\mathcal{A}} = \mathcal{A}'$.■

6 Rational basic set outside a maximal $\mathcal{A}$-ideal

In this section we prove Theorem 6.1 from which Theorem 1.2 immediately follows. Below a subset X of a ring R is called *Q-rational* for some $Q \subset \mathcal{P}(R)$ if $R_Q^\times X = X$. When $Q = \{p\}$, we say that X is p-rational.

Theorem 6.1 *Let $\mathcal{A}$ be an S-ring over a CG-ring R and $I \in \mathcal{I}_{max}(\mathcal{A})$. Suppose that any basic set in $\mathcal{S}(\mathcal{A})_{R \setminus I}$ is Q-rational where $Q = \mathcal{P}(R/I)$. Set $I^\star$ to be the intersection of all $\mathcal{A}$-ideals containing R_Q. Then the ring $\mathcal{A}$ satisfies the I/J-condition where $J = I \cap I^\star$. Moreover, if $J = 0$, then $\mathcal{A} = \mathcal{A}_I \otimes \mathcal{A}_{I^\star}$.*

The proof of the Theorem 6.1 will be given in the end of the section. In the following auxiliary statement we study some properties of the $\mathcal{A}$-ideals I, $I^\star$ and J defined in it. We keep the notations and the hypothesis of this theorem except for the Q-rationality.

Lemma 6.2 *The following statements hold:*

(1) $I + I^\star = R$, $I^\star = R_Q + J_{Q'}$ *and* $|R/I| = |I^\star/J| = |R_Q/J_Q|$,

(2) $\mathcal{I}_{max}(\mathcal{A}_{I^\star}) = \{J\}$,

(3) *for each $p \in Q$ the ideal $I^\star$ equals the intersection of all $\mathcal{A}$-ideals containing R_p,*

(4) $I_{\mathrm{L}}(X)_Q \subset J$ *for all* $X \in \mathcal{S}(\mathcal{A})_{R\setminus I}$.

Proof. By the definition of Q we have $R_Q \not\subset I$. Therefore $I^\star \not\subset I$, and $I + I^\star = R$ by the maximality of I. This gives the natural group isomorphism

$$I^\star/J \cong R/I \tag{21}$$

and hence $|R/I| = |I^\star/J|$. Since $\mathcal{P}(R/I) = Q$, it follows that $I^\star = R_Q + J_{Q'}$ and $|I^\star/J| = |R_Q/J_Q|$ which completes the proof of statement (1). Isomorphism (21) induces the bijection

$$\{I' \in \mathcal{I}(R) : \ J \subset I' \subset I^\star\} \to \{I' \in \mathcal{I}(R) : \ I \subset I' \subset R\}, \quad I' \mapsto I + I'$$

the converse to which takes I' to $I' \cap I^\star$. This induces a bijection on the $\mathcal{A}$-ideals. Thus statement (2) follows from the maximality of I. To prove statement (3) let $p \in Q$. Denote by I' the intersection of all $\mathcal{A}$-ideals containing R_p. Then obviously $I' \subset I^\star$. By statement (2) this implies that either $I' \subset J$ or $I' = I^\star$. Since $p \in \mathcal{P}(I^\star/J)$ (see statement (1)) and $R_p \subset I'$, the inclusion is impossible and we are done. Let us prove statement (4). Since $X \in \mathcal{S}(\mathcal{A})$ and $I \in \mathcal{I}_{max}(\mathcal{A})$, we see that $I_{\mathrm{L}}(X) \subset I$. On the other hand, $I_{\mathrm{L}}(X)_Q \subset R_Q \subset I^\star$. Thus $I_{\mathrm{L}}(X)_Q \subset I \cap I^\star = J$.■

In fact, Theorem 6.1 will be deduced from the following statement where we use the same notations.

Theorem 6.3 *Let $\mathcal{A}$ be an S-ring over a CG-ring R, $I \in \mathcal{I}_{max}(\mathcal{A})$ and $X \in \mathcal{S}(\mathcal{A})_{R\setminus I}$. Suppose that the set X is p-rational for some $p \in Q$. Then $J \subset I_{\mathrm{L}}(X)$ and*

$$\pi(X) = \pi(X)_Q + \pi(X)_{Q'} \tag{22}$$

where $\pi = \pi_J$. Moreover, both $\pi(X)_Q$ and $\pi(X)_{Q'}$ are basic sets of the S-ring $\mathcal{A}_{R/J}$, and $\pi(X)_Q = \pi(I^\star)^\#$.

Proof. By statement (4) of Lemma 6.2 without loss of generality we can assume that $I_{\mathrm{L}}(X)_p = 0$. First, we claim that

$$\mathrm{rk}(\mathcal{A}_{R/I}) = 2. \tag{23}$$

Indeed, the maximality of I implies that the S-ring $\mathcal{A}_{R/I}$ is R/I-primitive. Therefore (23) follows from Theorem 5.2 whenever the ring R/I is not a field. However, if it is a field, then $\mathcal{P}(R/I) = \{p\}$ and (23) follows from the p-rationality of X.

Let us prove that $J \subset I_{\mathrm{L}}(X)$. To do this we observe that from (23) it follows that $\pi_I(X) = \pi_I(R_Q)^\#$. So $X_p \neq \{0\}$. Since $R_p^\times X = X$, this implies by statement (3) of Theorem 5.3 that $I_{\mathrm{L}}(X \cup Y)_p \neq 0$ where Y is as in this theorem. Therefore

$$I_{\mathrm{L}}(X \cup Y) \supset I_0^\star \tag{24}$$

where $I_0^\star$ is the intersection of all $\mathcal{A}$-ideals I' with $I'_p \neq 0$. Clearly, $I_0^\star \in \mathcal{I}(\mathcal{A})$. Moreover, from the definition of $I^\star$ it follows that $I_0^\star \subset I^\star$. Therefore by statement (2) of Lemma 6.2 we have

$$I_0^\star = I^\star \quad \text{or} \quad I_0^\star \subset J. \tag{25}$$

Let $I' \subset I_0^\star$ be a non-zero $\mathcal{A}$-ideal of R other than $I^\star$. Then from (24) it follows that $Y + I' \subset X \cup Y$. On the other hand,

$$X \cap (Y + I') = \emptyset. \tag{26}$$

Indeed, otherwise $X \subset Y + I'$ because X is a basic set of $\mathcal{A}$ and $Y + I'$ is an $\mathcal{A}$-set. Since $X \in \mathcal{S}(\mathcal{A})_{R\setminus I}$ and $\mathrm{rk}(\mathcal{A}_{R/I}) = 2$, there exists $x \in X$ such that $x_p \in R_p^\times$. However, $(X^{[p]})_p = \{0\}$ by statement (1) of Theorem 5.3. So $Y_p = \{0\}$. Moreover, $I' \subset J$ by statement (2) of Lemma 6.2. Therefore from statement (1) of this lemma it follows that $R_p^\times \cap I' = \emptyset$. Thus $x \notin I'$. Contradiction. Thus (26) holds, and hence $Y + I' = Y$. But then using (24) we obtain that $I' \subset I_{\mathrm{L}}(X)$. This implies that

$$I_0^\star = I^\star. \tag{27}$$

Otherwise, $I_0^\star \subset J \neq I^\star$ and we can take $I' = I_0^\star$, which contradicts the assumption that $I_{\mathrm{L}}(X)_p = 0$. In this case we can take $I' = J$, which proves that $J \subset I_{\mathrm{L}}(X)$.

To complete the proof it suffices to assume that $J = 0$. Then $I^\star = R_Q$ and $I = R_{Q'}$. Since both of them are $\mathcal{A}$-ideals, we have $X_Q, X_{Q'} \in \mathcal{S}(\mathcal{A})$ (Lemma 2.2). Moreover, from statement (2) of Lemma 6.2 it follows that $X_Q = (R_Q)^\#$. Next, by (24) and (27) the set $X \cup Y$ is a union of R_Q-cosets. On the other hand, by the definition of Y we have $Y_{p'} \subset X_{p'}$, and hence $Y_{Q'} \subset X_{Q'}$. Thus

$$X \cup Y = R_Q + X_{Q'}. \tag{28}$$

However, since $X_Q = (R_Q)^\#$, we have $X \subset R_Q^\# + X_{Q'}$. On the other hand, $Y \subset X_{Q'}$, for otherwise $Y_Q \neq \{0\}$, and hence $Y_Q \supset R_Q^\#$ which contradicts the fact that $Y_p = \{0\}$. Thus from (28) it follows that $X = R_Q^\# + X_{Q'}$.∎

Proof of Theorem 6.1. Since the set $\mathcal{S}(\mathcal{A})_{R\setminus I}$ consists of Q-rational sets, we conclude by Theorem 6.3 that $J \subset I_{\mathrm{L}}(X)$ for all $X \in \mathcal{S}(\mathcal{A})_{R\setminus I}$. Thus the S-ring $\mathcal{A}$ satisfies the I/J-condition. To complete the proof suppose that $J = 0$. Then $I^\star = R_Q$ and $I = R_{Q'}$ where $Q' = \mathcal{P}(R) \setminus Q$. Therefore from Theorem 6.3 it follows that for all $X \in \mathcal{S}(\mathcal{A})_{R\setminus I}$ we have $X_Q \in \mathcal{S}(\mathcal{A}_I)$, $X_{Q'} \in \mathcal{S}(\mathcal{A}_{I^\star})$ and $X = X_Q + X_{Q'}$. Since these three relations obviously hold for $X \in \mathcal{S}(\mathcal{A})_I$, we are done.∎

7 S-rings with $\mathcal{I}_{max}(\mathcal{A}) \ne \mathcal{I}_{max}(R)$

It is known that any non-dense S-ring over a cyclic group is either a non-trivial generalized wreath product, or a tensor product one factor of which is an S-ring of rank 2 (see [4, Theorem 5.3]). In the case of S-rings over an arbitrary CG-ring we can prove the same statement only under a stronger condition yet.

Theorem 7.1 *Let $\mathcal{A}$ be an S-ring over a CG-ring R. Suppose that $\mathcal{I}_{max}(\mathcal{A}) \ne \mathcal{I}_{max}(R)$. Then $\mathcal{A}$ is either a non-trivial generalized wreath product, or a tensor product one factor of which is an S-ring of rank 2 over a non-field.*

Since $I \in \mathcal{I}_{max}(\mathcal{A})$ is a maximal ideal of R if and only if R/I is a field, Theorem 7.1 is an immediate consequence of the following statement in which we keep the notations of Section 6.

Theorem 7.2 *Let $\mathcal{A}$ be an S-ring over a CG-ring R and $I \in \mathcal{I}_{max}(\mathcal{A})$. Suppose that R/I is not a field. Then the ring $\mathcal{A}$ satisfies the I/J-condition. Moreover, if $J = 0$, then $\mathcal{A} = \mathcal{A}_I \otimes \mathcal{A}_{I^\star}$.*

In its turn Theorem 7.2 is an immediate consequence of Theorem 6.1 and the following statement which will be proved a bit later.

Theorem 7.3 *Let $\mathcal{A}$ be an S-ring over a CG-ring R and $I \in \mathcal{I}_{max}(\mathcal{A})$. Suppose that R/I is not a field. Then any basic set in $\mathcal{S}(\mathcal{A})_{R\setminus I}$ is Q-rational where $Q = \mathcal{P}(R/I)$.*

Proof. We need a special consequence of Theorem 6.3 that gives us a convenient form of a Q-rational basic set.

Lemma 7.4 *In the conditions of Theorem 6.3 we have $X = (R_Q \setminus J_Q) + X_{Q'}$.*

Proof. Since the full π-preimages of $\pi(X)$ and $\pi(X)_Q$ are X and $I^\star \setminus J$ respectively, from the equality (22) we obtain that

$$X = (I^\star \setminus J) + Y \tag{29}$$

where Y is the full preimage of $\pi(X)_{Q'}$. Taking into account that $Q \cap Q' = \emptyset$, we have $\pi(Y_Q) = \pi(Y)_Q = 0$, and hence $Y_Q \subset J_Q$. Therefore

$$J_Q + y = J_Q + y_Q + y_{Q'} = J_Q + y_{Q'}$$

for all $y \in Y$. Since Y is a union of J_Q-cosets, this shows that $Y = J_Q + Y_{Q'}$. On the other hand, $X_{Q'}$ and $Y_{Q'}$ are unions of $J_{Q'}$-cosets, and so $J_Q + X_{Q'}$ and $J_Q + Y_{Q'}$ are unions of J-cosets. Since also $\pi(X_{Q'}) = \pi(Y_{Q'})$, we have $J_Q + X_{Q'} = J_Q + Y_{Q'}$. Thus from (29) we obtain

$$X = (I^\star \setminus J) + Y = (I^\star \setminus J) + J_Q + Y_{Q'} = (I^\star \setminus J) + J_Q + X_{Q'} = (I^\star \setminus J) + X_{Q'}. \tag{30}$$

Finally, from statement (1) of Lemma 6.2 it follows that

$$I^\star \setminus J = (R_Q + J_{Q'}) \setminus (J_Q + J_{Q'}) = (R_Q \setminus J_Q) + J_{Q'}.$$

However, $X_{Q'}$ is a union of $J_{Q'}$-cosets. Thus we are done due to (30).■

Turn to the proof of Theorem 7.3. Let $X \in \mathcal{S}(\mathcal{A})_{R\setminus I}$ and $p \in Q$. Set $Y = R_p^\times X$. Then obviously $Y_{Q'} = X_{Q'}$. Therefore by Lemma 7.4 we have

$$Y = (R_Q \setminus J_Q) + X_{Q'}. \tag{31}$$

If $|Q| > 1$, then by statement (5) of Lemma 6.2 there exists an element of $R_Q \setminus J_Q$ with zero p-coordinate. Due to (31) one can find an element in Y, and hence in X, say x, with the same property. Then $x_p = 0$ and hence $R_p^\times x = x$. Therefore $R_p^\times X = X$. Thus the basic set X is Q-rational and we are done. In the remaining case $|Q| = 1$ we make use of the following lemma proved in Section 12.

Lemma 7.5 *Suppose that $Q = \{p\}$. Then*

(1) *if $p \notin \mathcal{P}(J)$, then $R_p^\times X = X$,*

(2) *if $p \in \mathcal{P}(J)$, then $I_{\mathrm{L}}(X) \cap J \neq 0$.*

To complete the proof let $Q = \{p\}$. Then by statement (1) of Lemma 7.5 we can assume that $p \in \mathcal{P}(J)$. In this case by statement (2) of that lemma $J_0 = I_{\mathrm{L}}(X) \cap J$ is a non-zero $\mathcal{A}$-ideal of R. Set $R' = \pi(R)$, $\mathcal{A}' = \mathcal{A}_{R'}$, $I' = \pi(I)$ and $X' = \pi(X)$ where $\pi = \pi_{J_0}$. Then obviously $I' \in \mathcal{I}(\mathcal{A}')$ and $X' \in \mathcal{S}(\mathcal{A}')_{R'\setminus I'}$. Moreover, since $J_0 \subset J \subset I$ we have

$$\mathcal{P}(R'/I') = \mathcal{P}(R/I) = Q = \{p\}.$$

Finally, $I_{\mathrm{L}}(X') \cap J' = 0$, and hence $p \notin \mathcal{P}(J')$ by statement (2) of Lemma 7.5. Thus from statement (1) of that lemma it follows that $(R'_p)^\times X' = X'$. Since X is a union of J_0-cosets, this implies that $R_p^\times X = X$.■

8 Decomposition of a pure S-ring

We note that not every pure S-ring over a CG-ring is dense, e.g. take the S-ring of rank 2 over a non-field. The following theorem shows that at least in the odd case this is essentially a unique reason for a pure S-ring not to be dense.

Theorem 8.1 *Any pure S-ring over a CG-ring of odd characteristic is the tensor product of a dense pure S-ring and S-rings of rank* 2 *over non-fields.*

We will prove Theorem 8.1 in the end of this section. In what follows we say that a pure S-ring is *indecomposable* if it is not a tensor product, one factor of which is an S-ring of rank 2 over a non-field.

Theorem 8.2 *Let $\mathcal{A}$ be an S-ring over a CG-ring R. Then the following statements are equivalent:*

(1) *$\mathcal{A}$ is pure indecomposable,*

(2) *$\widehat{\mathcal{A}}$ is pure indecomposable,*

(3) *$\mathcal{A}$ is pure and $\mathcal{I}_{max}(\mathcal{A}) = \mathcal{I}_{max}(R)$,*

(4) *$\mathcal{A}$ is pure and $\mathcal{I}_{min}(\mathcal{A}) = \mathcal{I}_{min}(R)$.*

Proof. From Theorem 5.8 it follows that if $\mathcal{A}$ or $\widehat{\mathcal{A}}$ is pure, then neither $\mathcal{A}$ nor $\widehat{\mathcal{A}}$ is a nontrivial generalized wreath product. Besides, it is easily seen that if $\mathcal{A}$ is a tensor product one factor of which is an S-ring of rank 2 over a non-field, then $\mathcal{I}(\mathcal{A}) \neq \mathcal{I}(R)$. By Theorem 7.1 these facts prove the equivalence (1) $\Leftrightarrow$ (3). To complete the proof of the theorem it suffices to verify the implication (1) $\Rightarrow$ (2). Indeed, if it is true, then the converse implication follows by duality, and the equivalence (3) $\Leftrightarrow$ (4) is an immediate consequence of the fact that $\mathcal{I}_{min}(R) = \mathcal{I}_{min}(\mathcal{A})$ if and only if $\mathcal{I}_{max}(\widehat{R}) = \mathcal{I}_{max}(\widehat{\mathcal{A}})$ (see (20)).

To prove the implication (1) $\Rightarrow$ (2) suppose that $\mathcal{A}$ is a pure indecomposable S-ring. Then by statement (2) of Theorem 2.5 and Theorem 7.1 it suffices to verify that $\widehat{\mathcal{A}}$ is a pure S-ring. For this purpose we note that due to the implication (1) $\Rightarrow$ (3), the set $R^\times$ being the complement in R to the union of all maximal $\mathcal{A}$-ideals, is an $\mathcal{A}$-subset of R. This implies that the basic set X of $\mathcal{A}$ that contains 1 is a subset of $R^\times$. Thus by Theorem 5.1 the set X is a subgroup of $R^\times$, which is pure by the hypothesis. Let $\chi \in \widehat{R}^\times$ and $\widehat{X}$ the basic set of $\widehat{\mathcal{A}}$ containing χ. It suffices to verify that $I_{\mathrm{L}}(\widehat{X}) = 0$. Suppose that this is not true. Then

$$\widehat{X}\chi' = \widehat{X}, \qquad \chi' \in I_{\mathrm{L}}(\widehat{X}). \tag{32}$$

Since the set X is pure, by statement (2) of Theorem 4.2 for $S = X$ we have $\chi(X') \neq 0$ where $X' = Xr$ for some $r \in R^\times$. Since $X' \in \mathcal{S}(\mathcal{A})$ from (32) we obtain that $\chi(X') = \chi\chi'(X')$ for all $\chi' \in I_{\mathrm{L}}(\widehat{X})$. So

$$a = \sum_{\chi' \in I_{\mathrm{L}}(\widehat{X})} \chi\chi'(X') \neq 0. \tag{33}$$

On the other hand, set $K = 1 + I$ where I is the preimage of the ideal $I_{\mathrm{L}}(\widehat{X})$ with respect to the isomorphism from R to $\widehat{R}$ induced by χ. Then when χ' runs over the set $I_{\mathrm{L}}(\widehat{X})$ the element $\chi\chi'$ runs over the set $\{\chi^{(r)} :\ r \in K\}$. Then

$$a = \sum_{r \in K} \chi^{(r)}(X') = \sum_{r \in K}\sum_{x \in X'} \chi^{(r)}(x) = \sum_{x \in X'}\sum_{r \in K} \chi(rx).$$

However $\chi(I) = 0$ because χ is non-trivial on I. Therefore for all $x \in R^\times$ we have

$$\sum_{r \in K} \chi(rx) = \sum_{h \in I} \chi(x + hx) = \chi(x)\sum_{h \in I} \chi(hx) = \chi(x)\chi(I) = 0.$$

Thus $a = 0$ because $X' \subset R^\times$, which contradicts (33).■

Theorem 8.3 *The S-ring dual to a pure S-ring over a CG-ring is also pure.*

Proof. By statement (2) of Theorem 2.5 without loss of generality we can assume that the input S-ring is indecomposable. Then the required statement immediately follows from the implication (1) ⇒ (2) of Theorem 8.2.■

Proof of Theorem 8.1. By statement (2) of Theorem 2.5 without loss of generality we can assume that the S-ring $\mathcal{A}$ is indecomposable. Therefore Theorem 8.1 is an immediate consequence of the following statement.

Theorem 8.4 *Suppose that the characteristic of a CG-ring R is odd. Then any pure indecomposable S-ring over R is dense.*

Proof. Let $\mathcal{A}$ be a pure indecomposable S-ring over the ring R. Suppose that R_p is not a field for some p. Denote by J the minimal ideal of R_p. Then by the implication (1) $\Rightarrow$ (4) of Theorem 8.2 we have $J \in \mathcal{I}(\mathcal{A})$. Since obviously $J \neq R_p$ and the characteristic of the ring R is odd, from Theorem 5.5 it follows that the S-ring $\mathcal{A}_{R/J}$ is pure. Moreover, it is easily seen that any maximal ideal of R/J is the π_J-image of a maximal ideal of R. Therefore by the equivalence (1) $\Leftrightarrow$ (3) of Theorem 8.2 the S-ring $\mathcal{A}_{R/J}$ is a pure indecomposable one. So by induction we conclude that $\mathcal{I}(\mathcal{A}_{R/J}) = \mathcal{I}(R/J)$. Thus $\mathcal{I}(\mathcal{A})$ contains any ideal I such that $I_p \neq 0$ for some $p \in \mathcal{P}$ for which R_p is not a field. Therefore by the implication (1) $\Rightarrow$ (4) of Theorem 8.2 we have $\mathcal{I}(\mathcal{A}) = \mathcal{I}(R)$.■

9 Dense pure S-rings

In this section we prove the following theorem which provides together with Theorem 8.1 a straightforward deduction of Theorem 1.3.

Theorem 9.1 *Any dense pure S-ring over a CG-ring of odd characteristic is cyclotomic.*

The proof will be given in the end of the section throughout which we fix a dense S-ring $\mathcal{A}$ over a CG-ring R. From equality (20) it follows that the ring $\widehat{\mathcal{A}}$ is also dense. We need two lemmas in each of which the characteristic of the ring R is arbitrary.

Lemma 9.2 *Suppose that* $\mathrm{Orb}(K, R^\times) \subset \mathcal{S}^*(\mathcal{A})$ *where* $K \leq R^\times$. *Then any pure orbit of the group* $\widehat{K}$ *in* $\widehat{R}$ *belongs to* $\mathcal{S}^*(\widehat{\mathcal{A}})$.

Proof. Let X_1 be a pure orbit of the group $\widehat{K}$. Then $X_1 = \chi_1^{\widehat{K}}$ for some character $\chi_1 \in \widehat{R}$. Denote by X the basic set of $\widehat{\mathcal{A}}$ containing χ_1 and set $X_2 = \chi_2^{\widehat{K}}$ where $\chi_2 \in X$. Since $\widehat{\mathcal{A}}$ is dense, the set $Y = \widehat{R}^\times \chi_1$ belongs to $\mathcal{S}^*(\widehat{\mathcal{A}})$ (see (16)). This implies that $X \subset Y$ whence it follows that $\chi_1, \chi_2 \in Y$, and hence $X_1, X_2 \subset Y$.

Denote by a the cardinality of the kernel of the natural action of the group K on the set Y. Since the action is semiregular (see Section 3), given $S \in \mathrm{Orb}(K, R^\times)$ and $s \in S$ we have

$$\chi_i(S) = \sum_{r \in K} \chi_i(rs) = \sum_{r \in K} \chi_i^{(r)}(s) = as(X_i), \quad i = 1, 2,$$

where $s(X_i)$ is defined by (1) with $G = \widehat{R}^+$, $S = X_i$ and χ being the character of G corresponding to s. On the other hand, as $S \in \mathcal{S}^*(\mathcal{A})$ the definition of the dual S-ring implies that $\chi_1(S) = \chi_2(S)$. Thus

$$s(X_1) = s(X_2), \quad s \in R^\times.$$

Since X_1 and X_2 are pure orbits of the group K, from statement (1) of Theorem 4.2 applied to $\widehat{R}$ and X_1, X_2 it follows that $X_1 = X_2$ and hence $\chi_2 \in X_1$. However, χ_2 is an arbitrary element of X. Thus $X \subset X_1$ and we are done.■

From now on we assume that for any $p \in \mathcal{P}$ where $\mathcal{P} = \mathcal{P}(R)$, the characteristic of the Galois ring R_p equals p^{n_p} for some $n_p \geq 1$. Set

$$\mathcal{P}' = \{p \in \mathcal{P} :\ n_p > 1\}, \qquad R' = \bigcup_{\mathcal{P}' \subset Q \subset \mathcal{P}} R_Q^\times. \tag{34}$$

Due to the density of $\mathcal{A}$, from (16) it follows that $R_Q^\times$ is $\mathcal{A}$-set for all Q, and hence $R' \in \mathcal{S}^*(\mathcal{A})$. Moreover, by Lemma 2.2 and the definition of $\mathcal{P}'$ we have

$$\mathcal{S}(\mathcal{A})_{R'} = \{X_Q :\ X \in \mathcal{S}(\mathcal{A})_{R^\times},\ Q \supset \mathcal{P}'\}. \tag{35}$$

Below for $p \in \mathcal{P}'$ we denote by $m(p)$ the product of all $q \in \mathcal{P}' \setminus \{p\}$.

Lemma 9.3 *Let $\mathcal{S}(\mathcal{A})_{R^\times} = \mathrm{Orb}(K, R^\times)$ where $K \leq R^\times$. Suppose that for some $p \in \mathcal{P}'$ the orbits of the group K on the set $pR^\times \cup m(p)R^\times$ are pure $\mathcal{A}$-sets. Then $\mathcal{S}(\mathcal{A})_{pR^\times} = \mathrm{Orb}(K, pR^\times)$.*

Proof. Suppose on the contrary that there is an orbit $X \in \mathrm{Orb}(K, pR^\times)$ containing two distinct basic sets Y and Y' of $\mathcal{A}$. Then

$$Y' = rY \tag{36}$$

for some $r \in K$. By the hypothesis of the lemma the sets X and $Z = mK$ with $m = m(p)$, are pure. Therefore, by Theorem 4.2 (with $S = Y$ and $S' = Y'$ for statement (1), and with $S = Z$ for statement (2)) there exist a character $\chi \in \widehat{R}$ and a set $Z' = r'Z$ with $r' \in R^\times$ such that

$$\chi(Y) \neq \chi(Y'), \quad \chi(Z') \neq 0. \tag{37}$$

However, by the definition of m we have $Y + Z' \subset R'$ where R' is the $\mathcal{A}$-set defined in (34). Since also $Y \in \mathcal{S}(\mathcal{A})$ and $Z' \in \mathrm{Orb}(K, mR^\times) \subset \mathcal{S}^*(\mathcal{A})$, we conclude that

$$\xi(Y)\xi(Z') \in \mathcal{A}_{R'}. \tag{38}$$

Taking into account that $\mathcal{S}(\mathcal{A})_{R^\times} = \mathrm{Orb}(K, R^\times)$ and that the set of K-orbits is closed with respect to taking projections, we see by (35) that the right-hand side of (38) is K-invariant. This implies that so is the left-hand side. Therefore by (36) and the definition of Z' we have

$$\xi(Y)\xi(Z') = r(\xi(Y)\xi(Z')) = \xi(rY)\xi(rZ') = \xi(Y')\xi(Z').$$

Applying χ to both sides of this equality we obtain a contradiction with (37).∎

Proof of Theorem 9.1. Let $\mathcal{A}$ be a dense pure S-ring over a CG-ring R of odd characteristic. Due to the density of $\mathcal{A}$, Theorem 5.1 implies that there exists a group $K \le R^\times$ such that

$$\mathcal{S}(\mathcal{A}) = \mathrm{Orb}(K, R^\times). \tag{39}$$

So by Lemma 9.2 any pure orbit of the group $\widehat{K}$ belongs to $\mathcal{S}^*(\widehat{\mathcal{A}})$. However, since the S-ring $\mathcal{A}$ is pure, the group K and hence the group $\widehat{K}$ are also pure. By Theorem 4.1 this implies that

$$\mathrm{Orb}(\widehat{K}, m\widehat{R}) \subset \mathcal{S}^*(\widehat{\mathcal{A}})_{m\widehat{R}} \tag{40}$$

for all integers m dividing $n/\prod_{p\in\mathcal{P}} p$. However, by Lemma 2.2 each basic set of $\widehat{\mathcal{A}}$ is the projection of some element of $\mathcal{S}(\widehat{\mathcal{A}})_{m\widehat{R}}$ with m as above. Therefore inclusion (40) holds for all m. Thus $\widehat{\mathcal{A}} \ge \mathrm{Cyc}(\widehat{K}, \widehat{R})$, and hence $\mathcal{A} \ge \mathrm{Cyc}(K, R)$ by Theorem 5.9. Since the group K is pure, this implies by (39) and Lemma 9.3 that

$$\mathcal{S}(\mathcal{A})_{pR^\times} = \mathrm{Orb}(K, pR^\times), \qquad p \in \mathcal{P}',$$

where $\mathcal{P}'$ is defined as in (34). Moreover, by Theorem 4.1 the group $K_{pR} = f_{pR}(K)$ where f_{pR} is the epimorphism defined in the end of Subsection 3.1 (see (7) and below), is a pure subgroup of the group $(R_{pR})^\times$ (here $K_{pR} = pK$ as sets, see (8)). So by induction we can assume that

$$\mathcal{S}(\mathcal{A})_{pR} = \mathrm{Cyc}(K_{pR}, R_{pR}), \qquad p \in \mathcal{P}'. \tag{41}$$

However, $\mathcal{S}(\mathcal{A}) = \mathcal{S}(\mathcal{A})_{R'} \cup \mathcal{S}'$ where R' is as in (34) and $\mathcal{S}' = \bigcup_{p\in\mathcal{P}'} \mathcal{S}(\mathcal{A})_{pR}$. Besides, due to (39) and (35) we have $\mathcal{S}(\mathcal{A})_{R'} \subset \mathrm{Orb}(K, R)$. Since by (41) we also have $\mathcal{S}' \subset \mathrm{Orb}(K, R)$, it follows that $\mathcal{S}(\mathcal{A}) \subset \mathrm{Orb}(K, R)$. Thus $\mathcal{A} = \mathrm{Cyc}(K, R)$.∎

10 Proof of Theorem 1.1

Denote by $\mathcal{T}_p$ and $\mathcal{U}_p$ (resp. by $\mathcal{T}_q$ and $\mathcal{U}_q$) the Teichmüller group and the group of principal units of the ring R_p (resp. R_q). Since q divides p^d-1, the cyclic group $\mathcal{T}_p$ of order p^d-1 contains a unique subgroup T_p of order q. Similarly, since p divides q^e-1, the cyclic group $\mathcal{T}_q$ of order q^e-1 contains a unique subgroup T_q of order p. Let us consider a subgroup of $R^\times$ defined as follows:

$$K=(T_p\mathcal{U}_p)\times(T_q\mathcal{U}_q).$$

Thus $K_p=T_p\mathcal{U}_p$ and $K_q=T_q\mathcal{U}_q$ (see Notation). Any group $L\le K$ with $L_p=K_p$ and $L_q=K_q$ (i.e. a subdirect product of K_p and K_q) is determined by means of an appropriate group L_0 and epimorphisms $f_p:K_p\to L_0$, $f_q:K_q\to L_0$ as follows:

$$L=\{(u,v)\in K:\ f_p(u)=f_q(v)\}.$$

Let us define subgroups K_1 and K_2 of the group K in the above way where f_p and f_q are fixed epimorphisms on a cyclic group L_0 of order q in the first case and of order p in the second one. Clearly, the sets $R^\times$ and $pR\cup qR$ are both K_1-invariant and K_2-invariant. Set

$$\mathcal{S}=\mathrm{Orb}(K_1,R^\times)\cup\mathrm{Orb}(K_2,pR\cup qR). \tag{42}$$

Then to prove Theorem 1.1 it suffices to verify the following statement.

Theorem 10.1 *The $\mathbb{Z}$-module $\mathcal{A}=\mathrm{span}_{\mathbb{Z}}\{\xi(X):\ X\in\mathcal{S}\}$ is a non-pure dense S-ring over the ring R. Moreover, this S-ring cannot be a non-trivial generalized wreath product.*

Before giving the proof of Theorem 10.1 let us cite some simple properties of the groups K, K_1 and K_2. The following statement is straightforward.

Lemma 10.2 *There exist direct decompositions $\mathcal{U}_p=U_p\cdot U_p'$ and $\mathcal{U}_q=U_q\cdot U_q'$ with cyclic groups U_p and U_q, such that*

$$K_1=(\mathcal{U}_p\times T_qU_q')\cdot L_1,\qquad K_2=(T_pU_p'\times\mathcal{U}_q)\cdot L_2 \tag{43}$$

where L_1 is a subdirect product of T_p and U_q of order q and L_2 is a subdirect product of U_p and T_q of order p, and both decompositions (43) are direct.■

From Lemma 10.2 it follows that

$$|K_1| = p^{d+1}q^e,\ I_{\mathrm{L}}(K_1) = pR_p, \qquad |K_2| = p^d q^{e+1},\ I_{\mathrm{L}}(K_2) = qR_q. \tag{44}$$

Moreover,

$$K_1 \cdot K_2 = K, \qquad K_1 \cap K_2 = (U'_p \times U'_q) \cdot L_1 \cdot L_2$$

where the latter decomposition is direct, and for $i, j \in \{0, 1, 2\}$ we have

$$\mathrm{Orb}(K, p^i q^j R^\times) = \mathrm{Orb}(K_1, p^i q^j R^\times) = \mathrm{Orb}(K_2, p^i q^j R^\times), \qquad i+j \in \{2, 3, 4\}, \tag{45}$$

whereas if $(i, j) = (0, 1)$ or $(i, j) = (1, 0)$, then

$$\mathrm{Orb}(K, qR^\times) = \mathrm{Orb}(K_1, qR^\times), \qquad \mathrm{Orb}(K, pR^\times) = \mathrm{Orb}(K_2, pR^\times). \tag{46}$$

Proof of Theorem 10.1. Obviously, the elements of the set $\mathcal{S}$ form a partition of R such that any ideal of R is a union of classes of the partition. Moreover, the induced partition of $R^\times$ consists of orbits of the group K_1 which is not pure. Since also $R^\times \mathcal{S} = \mathcal{S}$, to prove the first of the theorem it suffices to verify that $\mathcal{A}$ is an S-ring over the group R^+.

From the definition of $\mathcal{S}$ it follows that $\{0\} \in \mathcal{S}$ and $-\mathcal{S} = \mathcal{S}$. Therefore we need to check only that $\xi(X)\xi(Y) \in \mathcal{A}$ for all $X, Y \in \mathcal{S}$. We distinguish three cases depending on to which parts of $\mathcal{S}$ the sets X and Y belong. Denote by ξ_1 and ξ_2 the elements of $\mathbb{Z}R$ such that

$$\xi(X)\xi(Y) = \xi_1 + \xi_2, \quad \mathrm{Supp}(\xi_1) \subset R^\times, \quad \mathrm{Supp}(\xi_2) \subset pR \cup qR.$$

Below for $\xi \in \mathbb{Z}R$ we set $I_{\mathrm{L}}(\xi)$ to be the largest ideal $I \in \mathcal{I}(R)$ for which $\xi\xi(I) = |I|\xi$; obviously, if $\xi = \xi(Z)$ for some $Z \subset R$, then $I_{\mathrm{L}}(\xi) = I_{\mathrm{L}}(Z)$.

Case 1: $X, Y \in \mathrm{Orb}(K_1, R^\times)$. In this case $\xi(X), \xi(Y) \in \mathrm{Cyc}(K_1, R)$, and hence $\xi_1, \xi_2 \in \mathrm{Cyc}(K_1, R)$. Thus since $K \geq K_2$, it suffices to verify that $\xi_2 \in \mathrm{Cyc}(K, R)$. However, since obviously $\xi(qR) \in \mathrm{Cyc}(K_1, R)$, from (45) and (46) it follows that $\xi_2 \circ \xi(qR) \in \mathrm{Cyc}(K, R)$. It remains to show that the element $\xi = \xi_2 \circ \xi(pR)$ belongs to $\mathrm{Cyc}(K, R)$. To do this we observe that by (44) we have $I_{\mathrm{L}}(X) = I_{\mathrm{L}}(Y) = pR_p$. Therefore $I_{\mathrm{L}}(\xi(X)\xi(Y)) \geq pR_p$ and hence

$$I_{\mathrm{L}}(\xi) \geq pR_p.$$

This implies that $\xi = \xi(pR_p)\xi'$ for some $\xi' \in \mathbb{Z}R_q$. In particular, all elements of each pR_p-coset enter ξ with the same coefficient. Therefore taking into account that $\xi \in \mathrm{Cyc}(K_1, R)$, we conclude that $\xi' \in \mathrm{Cyc}(K, R)$. Since also $\xi(pR_p) \in \mathrm{Cyc}(K, R)$, we obtain that $\xi \in \mathrm{Cyc}(K, R)$.

Case 2: $X, Y \in \mathrm{Orb}(K_2, pR \cup qR)$. Arguing as above we obtain that $\xi_1, \xi_2 \in \mathrm{Cyc}(K_2, R)$. Therefore without loss of generality we can assume that $\xi_1 \neq 0$ (see (42)). Then it is easily seen that $\xi_2 = 0$. Moreover, we can assume that $X \subset p^i R^\times$ and $Y \subset q^j R^\times$ where $i, j \in \{1, 2\}$. It suffices to verify that

$$\xi_X, \xi_Y \in \mathrm{Cyc}(K, R), \qquad I_{\mathrm{L}}(\xi_Y) = pR_p \tag{47}$$

where $\xi_X = \xi(pR_p)\xi(X)$ and $\xi_Y = \xi(qR_q)\xi(Y)$. Indeed, since $I_{\mathrm{L}}(K_2) = qR_q$, it follows that $I_{\mathrm{L}}(X) \geq qR_q$. The converse inclusion is obvious. Thus $I_{\mathrm{L}}(X) = qR_q$. Therefore using the second part of (47) we obtain that

$$\xi(X)\xi(Y) = (c_q\xi(X)\xi(qR_q))\xi(Y) = c_q\xi(X)(\xi(qR_q)\xi(Y)) = c_q\xi(X)\xi_Y =$$

$$c_q\xi(X)(c_p\xi(pR_p)\xi_Y) = c_pc_q(\xi(pR_p)\xi(X))\xi_Y = c_pc_q\xi_X\xi_Y$$

where $c_p = |pR_p|^{-1}$ and $c_q = |qR_q|^{-1}$. Thus $\xi_X\xi_Y \in \mathrm{Cyc}(K, R)$ by the first part of (47).

To prove (47) let $X = p^i u K_2$ for some $u \in R^\times$. By Lemma 10.2 we have $K_2 = (T_pU'_p \times \mathcal{U}_q) \cdot L_2$ and $L_2 = \{(f(t), t) : \ t \in T_q\}$ where $f : T_q \mapsto U_p$ is a group isomorphism. Therefore

$$p^i L_2 = \{(p^i f(t), p^i t) : \ t \in T_q\} = \{p^i\} \times p^i T_q,$$

and

$$X = (u_pT_pU'_p \times u_q\mathcal{U}_q) \cdot p^i L_2 = (u_pT_pU'_p \times u_q\mathcal{U}_q) \cdot (\{p^i\} \times p^i T_q) = p^i u_p T_p \times p^i u_q T_q \mathcal{U}_q.$$

So $\xi_X = \xi(pR_p)\xi(X) = c\,\xi(pR_p \times p^i u_q T_q \mathcal{U}_q)$ for a positive integer c. Thus $\xi_X \in \mathrm{Cyc}(K, R)$.

Next, let $Y = q^j u K_2$ where $u \in R^\times$. Then as above we have

$$Y = (q^j u_p T_p U'_p \times q^j u_q \mathcal{U}_q) \cdot L_2 = \bigcup_{t \in T_q} Z_t \times \{q^j u_q t\} \tag{48}$$

where $Z_t = q^j u_p f(t) T_p U'_p$. Since obviously $\xi(qR_q)\xi(Z_t \times \{q^j u_q t\}) = \xi(Z_t \times qR_q)$, this implies that

$$\xi_Y = \xi(qR_q)\xi(Y) = \sum_{t \in T_q} \xi(Z_t \times qR_q) =$$

$$\sum_{r\in U_p}\xi(q^j u_p r T_p U'_p \times qR_q) = \xi(q^j u_p T_p \mathcal{U}_p \times qR_q).$$

Thus $\xi_Y \in \mathrm{Cyc}(K,R)$. Since $q^j u_p T_p \mathcal{U}_p = q^j u_p T_p + pR_p$, we also obtain that $I_{\mathrm{L}}(\xi_Y) = pR_p$.

Case 3: $X \in \mathrm{Orb}(K_1, R^\times)$**,** $Y \in \mathrm{Orb}(K_2, pR \cup qR)$ (or vice versa). First, suppose that $Y \in \mathrm{Orb}(K_2, pR)$. Then from (45) and the second equality of (46) it follows that $Y \in \mathrm{Orb}(K, pR)$, and hence $\xi(Y) \in \mathrm{Cyc}(K_1, R)$. This implies that $\xi(X)\xi(Y) \in \mathrm{Cyc}(K_1, R)$. Therefore $\xi_1 \in \mathcal{A}$. Since also $\mathrm{Supp}(\xi_2) \subset qR$, by (45) and the first equality of (46) we conclude that $\xi_2 \in \mathrm{Cyc}(K,R) \subset \mathcal{A}$. Thus $\xi(X)\xi(Y) \in \mathcal{A}$.

Suppose that $Y \in \mathrm{Orb}(K_2, qR\backslash pR)$. Then $Y = q^j u K_2$ where $u \in R^\times$ and $j \in \{1,2\}$. The element Z_t defined in Case 2 can be rewritten in the following form: $Z_t = \bigcup_{s\in T_p}(r_t s + r_t s H)$ where $r_t = qu_p f(t)$ and $H = U'_p - 1 \subset pR_p$. However, for any $s \in T_p$ we have

$$\xi(r_t s + r_t sH)\xi(pR_p) = |H|\xi(r_t s + pR_p) = |H|\xi(r_t s\mathcal{U}_p) = |H|\xi(qu_p s\mathcal{U}_p).$$

Together with (48) this implies that

$$\xi(Y)\xi(pR_p) = \xi(\bigcup_{t\in T_q} Z_t \times \{qu_q t\})\xi(pR_p) =$$

$$(\sum_{t\in T_q}\xi(Z_t \times \{qu_q t\})\xi(pR_p) = \sum_{t\in T_q}\sum_{s\in T_p}\xi(r_t s + r_t sH)\xi(pR_p)\xi(qu_q t) =$$

$$|H|\sum_{s\in T_p}\sum_{t\in T_q}\xi(qu_p s\mathcal{U}_p)\xi(qu_q t) = |H|\xi(qu_p T_p \mathcal{U}_p \times qu_q T_q).$$

Thus $\xi(Y)\xi(pR_p) \in \mathrm{Cyc}(K,R)$. Besides, since $I_{\mathrm{L}}(X) = pR_p$, we have

$$\xi(X)\xi(Y) = c\,\xi(X)(\xi(Y)\xi(pR_p))$$

where c is a positive rational. Therefore $\xi(X)\xi(Y) \in \mathrm{Cyc}(K_1, R)$, whence it follows that $\xi_1, \xi_2 \in \mathrm{Cyc}(K_1, R)$. In particular, $\xi_1 \in \mathcal{A}$. To prove that $\xi_2 \in \mathcal{A}$, it suffices to verify that $\xi_2 \in \mathrm{Cyc}(K,R)$. However, it is easy to see that $\mathrm{Supp}(\xi_2) \subset pR$. Moreover, $I_{\mathrm{L}}(\xi_2) \geq pR_p$ because $\mathrm{Supp}(\xi_1) \cap pR = \emptyset$ and $I_{\mathrm{L}}(\xi(X)\xi(Y)) \geq I_{\mathrm{L}}(X) = pR_p$. Thus applying to $\xi = \xi_2$ the same argument as in the end of Case 2, we obtain that $\xi_2 \in \mathrm{Cyc}(K,R)$ which completes the proof of Case 3 and the first part of the theorem.

To prove the second part of the theorem suppose on the contrary that the S-ring $\mathcal{A}$ satisfies the I/J-condition non-trivially. Then without loss of generality we can assume that I is a maximal $\mathcal{A}$-ideal of R, i.e. $I = pR$ or $I = qR$. Since $R^\times \subset R \setminus I$ and $I_{\rm L}(X) = pR_p$ for all $X \in \mathcal{S}(\mathcal{A})_{R^\times}$ due to (44), we also can assume that $J = pR_p$. Suppose that $I = pR$. Then the set $X = qK_2$ belongs to $\mathcal{S}(\mathcal{A})_{R\setminus I}$, and hence $J \le I_{\rm L}(X)$. So $I_{\rm L}(X)_p \ne 0$. On the other hand, a straightforward computation based on Lemma 10.2 shows that $I_{\rm L}(X)_p = 0$. Contradiction. Finally, suppose that $I = qR$. Then the set $X = pK_2$ belongs to $\mathcal{S}(\mathcal{A})_{R\setminus I}$, and hence $I_{\rm L}(X)_p \ne 0$. On the other hand, $I_{\rm L}(X)_p = 0$ because X cannot contain any pR_p-coset. Contradiction.■

11 Proof of Theorem 4.2

The proof is based on the following two results on abelian groups to be proved in the end of the section. Let us fix some notation for an abelian group G. Denote by G_0 the socle of G; in our case it is the product of all subgroups of G of prime order. For $p \in \mathcal{P}$ and $Q \subset \mathcal{P}$ where $\mathcal{P} = \mathcal{P}(G)$, we set $G_{0,p} = (G_0)_p$ and $G_{0,Q} = (G_0)_Q$.

Theorem 11.1 *Let G be an abelian group of exponent m each Sylow p-subgroup of which is homocyclic and let $K \subset \mathbb{C}$ be a field linearly separated from $\mathbb{Q}[w]$ over $\mathbb{Q}$ where w is a primitive mth root of unity. Denote by $\Psi = \Psi_K(G)$ the set of all K-epimorphisms $\psi : KG \to K[w]$. Then*

$$\bigcap_{\psi\in\Psi} \ker(\psi) = I_K(G) \tag{49}$$

where $I_K(G) = \sum_{p\in\mathcal{P}} I_p \otimes KG_{p'}$ and I_p is the ideal of KG_p spanned by $\xi(G_{0,p})$.[5]

Lemma 11.2 *In the notation of Theorem 11.1 given a nonzero $\xi \in I_K(G)$ there exists a nonempty set $Q \subset \mathcal{P}$ and a $G_{0,Q}$-coset $A \subset G$ such that* $\mathrm{Supp}(\xi_A)_p \supset A_p$ *for all $p \in Q$ where $\xi_A = \xi \circ \xi(A)$.*

Let us turn to the proof of Theorem 4.2. By the hypothesis there exist a group $L \le R^\times$ and a pure orbit T of it such that $S, S' \subset T$. To prove

[5] Here and below all tensor products are taken over K.

statement (1) suppose on the contrary that $\chi(S) = \chi(S')$ for all $\chi \in \widehat{R}^{\times}$. However, when a character χ runs over $\widehat{R}^{\times}$ its extension $\psi : \mathbb{Q}G \to \mathbb{C}$ where $G = R^{+}$, runs over the set $\Psi_{\mathbb{Q}}(G)$ defined in Theorem 11.1. Thus $\xi(S) - \xi(S') \in \ker(\psi)$ for all $\psi \in \Psi_{\mathbb{Q}}(G)$. Since each Sylow subgroup of G is homocyclic in our case, by Theorem 11.1 this implies that $\xi(S) - \xi(S') \in I_K(G)$. Let us prove that this contradicts the purity of T.

Since $S \neq S'$ the element $\xi = \xi(S) - \xi(S')$ is nonzero. So by Lemma 11.2 there exist a nonempty set $Q \subset \mathcal{P}$ and a $G_{0,Q}$-coset $A \subset G$ such that $\mathrm{Supp}(\xi_A)_p \supset A_p$ for all $p \in Q$. Since $S, S' \subset T$, this implies that

$$(T \cap A)_p = A_p, \qquad p \in Q. \tag{50}$$

One can see that $T \cap A$ is a block of the abelian group L acting on T. This implies that $T \cap A \in \mathrm{Orb}(L')$ where L' is the setwise stabilizer of $T \cap A$ in L. Therefore

$$|T \cap A| = |L_A| \tag{51}$$

where L_A is the permutation group on $T \cap A$ induced by L'. It is easily seen that given $p \in Q$ the family M_p of all nonempty sets $X \cap T$, $X \in A/G_{0,Q\setminus\{p\}}$, forms an imprimitivity system for L_A. From (50) it follows that $|M_p| = |G_{0,p}|$ for all $p \in Q$. Besides, due to (51) the number $|M_p|$ divides $|T \cap A|$ for all $p \in Q$. Thus

$$|T \cap A| \geq \prod_{p \in Q} |G_{0,p}| = |A|$$

whence it follows that $T \supset A$. Therefore $T = T + G_{0,Q}$, and hence the set T is not pure. This contradiction completes the proof of statement (1).

To prove statement (2) let $\chi \in \widehat{R}^{\times}$. By statement (1) with $S' = \emptyset$ there exists a character $\chi' \in \widehat{R}^{\times}$ such that $\chi'(S) \neq \chi'(S') = 0$. However, due to (10) we have $\chi' = \chi^{(r)}$ for some $r \in R^{\times}$. Thus, $\chi(rS) = \chi'(S) \neq 0.$■

Proof of Theorem 11.1. Clearly, the right-hand side of (49) is contained in the left-hand side. Let us prove the converse inclusion by induction on $|\mathcal{P}|$. Without loss of generality we assume that $|\mathcal{P}| > 0$. Fix $q \in \mathcal{P}$ and set $G' = G_{q'}$ Then each $g \in G$ can uniquely be written in the form $g = g'g_q$ where $g' \in G'$ and $g_q \in G_q$.

For induction purposes some preliminary work is needed. Set $K' = K[w_q]$ where w_q is a primitive m_qth root of unity. For $\xi = \sum_{g \in G} a_g g$ belonging to KG and $\psi_q \in \Psi_K(G_q)$ define an element $\xi' = \xi'(\psi_q)$ of the ring $K'G'$ by

$$\xi' = \sum_{g' \in G'} a'_{g'} g' \quad \text{with} \quad a'_{g'} = \sum_{g_q \in G_q} a_{g' g_q} \psi_q(g_q).$$

Next, using the equalities $KG = KG' \otimes KG_q$ and $KG' \otimes K' = K'G'$ let us define a ring epimorphism

$$\widetilde{\psi}_q : KG \to K'G'$$

by $\widetilde{\psi}_q = \mathrm{id}_{KG'} \otimes \psi_q$. Then it is easily seen that

$$\widetilde{\psi}_q(\xi) = \xi', \quad \ker(\widetilde{\psi}_q) = KG' \otimes \ker(\psi_q), \quad \widetilde{\psi}_q(I_K(G') \otimes KG_q) = I_{K'}(G'). \tag{52}$$

To prove that the left-hand side of (49) is contained in the right-hand side suppose that $\xi \in \bigcap_{\psi \in \Psi} \ker(\psi)$. First, we claim that

$$\xi'(\psi_q) \in I_{K'}(G') \quad \text{for all } \psi_q \in \Psi_K(G_q). \tag{53}$$

Indeed, let $\psi_q \in \Psi_K(G_q)$. We note that the field K' is linearly separated from $\mathbb{Q}[w']$ over $\mathbb{Q}$ where w' is a primitive $m_{q'}$th root of unity because K is linearly separated from $\mathbb{Q}[w]$ over $\mathbb{Q}$. Therefore by the induction hypothesis for the group G' and the field K' it suffices to check that $\psi'(\xi') = 0$ for all $\psi' \in \Psi'$ where $\xi' = \xi'(\psi_q)$ and $\Psi' = \Psi_{K'}(G')$. However,

$$\psi'(\xi') = \psi'(\sum_{g' \in G'} a'_{g'} g') = \psi'(\sum_{g' \in G'} \sum_{g_q \in G_q} a_{g' g_q} \psi_q(g_q) g') =$$

$$\sum_{g' \in G'} \sum_{g_q \in G_q} a_{g' g_q} \psi'(g') \psi_q(g_q) = \sum_{g' \in G'} \sum_{g_q \in G_q} a_{g' g_q} \psi(g' g_q) = \sum_{g \in G} a_g \psi(g) = \psi(\xi)$$

where $\psi = \psi'_{KG'} \otimes \psi_q \in \Psi$ with $\psi'_{KG'}$ being the restriction of ψ' to KG'). By the choice of ξ, we conclude that $\psi'(\xi') = \psi(\xi) = 0$, and we are done.

Further, set $M = I_K(G') \otimes KG_q$ and $N_{\psi_q} = KG' \otimes \ker(\psi_q)$ where $\psi_q \in \Psi_K(G_q)$. Then from (52) and (53) it immediately follows that for all ψ_q we have

$$\xi \in (\widetilde{\psi}_q)^{-1}(\xi') \subset (\widetilde{\psi}_q)^{-1}(I_{K'}(G')) \subset M + \ker(\widetilde{\psi}_q) = M + N_{\psi_q}.$$

Therefore to complete the proof, i.e. to verify that $\xi \in I_K(G)$ it suffices to show that

$$\bigcap_{\psi_q \in \Psi_K(G_q)} (M + N_{\psi_q}) = I_K(G). \tag{54}$$

To prove (54) we observe that

$$(M + N_{\psi_q})/M = N_{\psi_q}/(M \cap N_{\psi_q}) =$$

$$N_{\psi_q}/(I_K(G') \otimes \ker(\psi_q)) = (KG'/I_K(G')) \otimes \ker(\psi_q).$$

On the other hand, from [8] it follows that $\bigcap_{\psi_q \in \Psi_K(G_q)} \ker(\psi_q) = I_K(G_q)$. Thus,

$$\bigcap_{\psi_q \in \Psi_K(G_q)} (M + N_{\psi_q})/M = (KG'/I_K(G')) \otimes I_K(G_q). \tag{55}$$

Similarly,

$$I_K(G)/M = (M + KG' \otimes I_K(G_q))/M = (KG'/I_K(G')) \otimes I_K(G_q). \tag{56}$$

Therefore (54) follows from (55) and (56).■

Proof of Lemma 11.2. Denote by M the set of all $Q \subset \mathcal{P}$ for which there exists a $G_{0,Q}$-coset A such that

$$\xi_A \in \mathrm{span}_K\{\xi(a + G_{0,p}) : \ a \in A, \ p \in Q\}^{\#}. \tag{57}$$

From the definition of $I_K(G)$ it follows that ξ is a K-linear combination of elements $\xi(a + G_{0,p})$ with $a \in G$ and $p \in \mathcal{P}$. Since also $\xi \neq 0$, we see that $\mathcal{P} \in M$. Let Q be a minimal (by inclusion) subset of $\mathcal{P}$ belonging to M and A the corresponding coset. Then obviously $Q \neq \emptyset$. We claim that for Q and A the statement of the theorem holds. Suppose on the contrary that this is not true. Then there exists $p \in Q$ such that $\mathrm{Supp}(\xi_A)_p \supsetneq A_p$. This implies that

$$\mathrm{Supp}(\xi_A) \cap B = \emptyset \tag{58}$$

for some coset $B \in A/G_{0,Q\setminus\{p\}}$. However, it is easily seen that given $b \in B$ and $q \in Q \setminus \{p\}$ we have

$$\xi(b + G_{0,q}) = \sum_{x \in G_{0,q}} \xi(b + x + G_{0,p}) - \sum_{y \in G_{0,p}^{\#}} \xi(b + y + G_{0,q}).$$

Therefore, without loss of generality we can assume that in a representation of ξ_A afforded by (57) the coefficient at $\xi(b + G_{0,q})$ equals 0 for all $b \in B$. Due to (58) this implies that the coefficient at $\xi(a + G_{0,p})$ equals 0 for all $a \in A$. Thus condition (57) holds for Q and A replaced by $Q \setminus \{p\}$ and any $G_{0,p}$-coset in A that intersects $\mathrm{Supp}(\xi_A)$, respectively. But this contradicts the minimality of Q.■

12 Proof of Lemma 7.5

From the assumptions it follows that $R_p = \mathrm{GR}(p^n, d)$ where $n \geq 2$.

Lemma 12.1 *Suppose that $R_q \subset J$ for some $q \in \mathcal{P}(R)$. Then $R_q \subset I_{\mathrm{L}}(X)$.*

Proof. Clearly, $q \neq p$. By Theorem 6.3 the set $R_p^\times X$ is a union of J-cosets. Due to the assumption each of them contains an element with zero q-coordinate. So the set X also contains such an element. Therefore $R_q^\times X = X$, and hence by statement (2) of Theorem 5.3 (for $p = q$)

$$I_{\mathrm{L}}(X)_q \neq 0 \quad \text{or} \quad X^{[q]} \neq \emptyset.$$

In the former case $(I_{\mathrm{L}}(X) \cap J)_q = I_{\mathrm{L}}(X)_q \neq 0$ and we are done by induction. Let us show that the latter case is impossible. Indeed, let us consider the $\mathcal{A}$-ideal

$$I' = I_{\mathrm{U}}(X^{[q]}) \cap I^\star.$$

Since $X \subset R \setminus I$ and $Q = \{p\}$, we have $x_p \notin J$ for all $x \in X$. However, $q \neq p$ and hence $x_p \notin J$ for all $x \in X^{[q]}$. This implies that $I_{\mathrm{U}}(X^{[q]})_p \not\subset J_p$. Since $I^\star \supset R_p$, it follows that $I'_p \not\subset J_p$. Therefore $I' \not\subset J$. By statement (2) of Lemma 6.2 this shows that $I' = I^\star$. Thus $I'_q = I^\star_q \supset J_q = R_q$. On the other hand, taking into account that $(X^{[q]})_q = \{0\}$ (statement (1) of Theorem 5.3), we see that $I'_q = 0$. Contradiction.■

Corollary 12.2 *If $p \notin \mathcal{P}(J)$, then $I^\star \setminus J \in \mathcal{S}(\mathcal{A})$.*

Proof. It is easily seen that the hypothesis of Lemma 7.5 is satisfied for $\mathcal{A}$, R and I replaced with $\mathcal{A}_{I^\star}$, $R_{I^\star}$ and J (see Lemma 6.2). Moreover, since $p \notin \mathcal{P}(J)$, we have $(R_{I^\star})_q \subset J$ for all $q \in \mathcal{P}(R_{I^\star})$, $q \neq p$. By Lemma 12.1 this implies that $(R_{I^\star})_q \subset I_{\mathrm{L}}(X)$ for all q and any $X \in \mathcal{S}(\mathcal{A}_{I^\star \setminus J})$. In particular, $J \leq I_{\mathrm{L}}(X)$. Since by statement (2) of Lemma 6.2 and Theorem 5.2 we have $\mathrm{rk}(\mathcal{A}_{I^\star/J}) = 2$, this implies that $X = I^\star \setminus J$ and we are done.■

Let us turn to the proof of Lemma 7.5. To prove statement (1) suppose that $p \notin \mathcal{P}(J)$. Denote by t the cardinality of the set $\{uX : \ u \in R_p^\times\}$. Then it suffices to verify that $t = 1$. To do this we observe that from Lemma 7.4 it follows that for any $x' \in X_{p'}$ the cardinality of the set

$$F_{x'} = \{x_p : \ x \in X, \ x_{p'} = x'\}$$

equals $f = |R_p^\#|/t$. Next, by Corollary 12.2 we have $I^\star \setminus J \in \mathcal{S}(\mathcal{A})$, and hence

$$\xi(X)\xi(-X) = \alpha\xi(I^\star \setminus J) + \xi'$$

where α is a non-negative integer and $\xi' \circ \xi(I^\star \setminus J) = 0$. It is easily seen that the element $x - y$ with $x, y \in X$ belongs to $I^\star \setminus J$ if and only if $x_p \neq y_p$ and $x_{p'} - y_{p'} \in J$. Since $|I^\star \setminus J| = |J||R_p^\#|$, it follows that

$$\alpha \leq f^2|X_{p'}||J|/|I^\star \setminus J| = f|X_{p'}|/t. \qquad (59)$$

On the other hand, taking into account that $p \notin \mathcal{P}(J)$ one can find $x_0 \in X$ such that $(x_0)_p$ is of order p. Since $(1 + \mathrm{rad}(R_p))\{x_0\} = \{x_0\}$, we have $(1 + \mathrm{rad}(R_p))X = X$. Besides, by Lemma 7.4 it is also true that

$$|F_{x'} \cap p^i R_p| = |p^i R_p^\times|/t, \qquad i = 0, \ldots, n-1,\ x' \in X_{p'}. \qquad (60)$$

Therefore the set $F_{x'} \setminus p^{n-1}R_p$ is a union of $p^{n-1}R_p$-cosets. This implies that given $x' \in X_{p'}$ an element of $I^\star \setminus J$ of order p can be represented as $x - y$ with $x, y \in X$, $x_{p'} = x'$ in at least $|F_{x'} \setminus p^{n-1}R_p| = f - f_0$ ways where $f_0 = |F_{x'} \cap p^{n-1}R_p| = |(p^{n-1}R_p)^\#|/t$ (see (60)). This implies that

$$\alpha \geq |X_{p'}|(f - f_0).$$

Together with (59) this shows that $f \geq tf - tf_0$ whence it follows that $|R_p^\#| \geq t(|R_p| - |p^{n-1}R_p|)$. Since $|R_p| = p^{nd}$ and $|p^{n-1}R_p| = p^d$, this gives $p^{nd} > t(p^{nd} - p^d)$. For $t \geq 2$ we have $p^{(n-1)d} < t/(t-1) \leq 2$, which is impossible for $n \geq 2$. Thus $t = 1$ and statement (1) is proved.

To prove statement (2) suppose that $p \in \mathcal{P}(J)$. By Lemma 12.1 we can assume that $R_q \not\subset J$ for all $q \in \mathcal{P}(R)$. It suffices to verify that

$$(1 + \mathrm{rad}(R_p))X = X. \qquad (61)$$

Indeed, we have $I_p = J_p$ by the lemma hypothesis and the definition of J, and $J_p \neq 0$ because $p \in \mathcal{P}(J)$. Therefore $I_p \neq 0$, and hence $X_p \subset R_p \setminus I_{0,p}$. Due to (61) this implies that the set X is a union of $I_{0,p}$-cosets. So $I_{\mathrm{L}}(X)_p \neq 0$ and we are done because $J_p \supset I_{0,p}$. To prove (61) we note that by the assumption $1 + J$ is a subgroup of $R^\times$. Then the set

$$Y = (1 + J)X$$

belongs to $\mathcal{S}^*(\mathcal{A})$. It is easily seen that the hypothesis of Lemma 7.5 is satisfied for $\mathcal{A}$ and X replaced with $\mathcal{A}_{R/J}$ and $\pi_J(Y)$. So by already proved statement (1) of this lemma we have $\pi_J(Y) = \pi_J(Y')$ for all $Y' \in M$ where $M = \{rY : \ r \in R_p^\times\}$. Therefore for any $y \in R$ the sets $Y_{J,y}$ and $Y'_{J,y}$ are empty or not simultaneously. By Lemma 2.1 this implies that

$$|Y_{J,y}| = |Y'_{J,rY}| = |Y'_{J,y}|$$

where $Y' = rY$. On the other hand, by Theorem 6.3 applied to $R_p^\times Y$ the full π_J-preimage of $\pi_J(R_p^\times Y)$ coincides with the union of all sets from M. This implies that given $y \in Y$ the set $y + J$ is a disjoint union of the sets $Y'_{J,y}$, $Y' \in M$. Thus

$$|J| = |y + J| = \sum_{Y' \in M} |Y'_{J,y}| = |M||Y_{J,y}|. \tag{62}$$

Next, take $y \in Y$ such that $y_p \in R_p^\times$ (such an y exists because $X \in \mathcal{S}(\mathcal{A})_{R \setminus I}$ and $Q = \{p\}$). Since $J_p \subset \mathrm{rad}(R_p)$, it follows that $y'_p \in R_p^\times$ for all $y' \in Y_{J,y}$. This implies that $|(1 + J_p)y'| = |J_p|$ for all $y' \in Y_{J,y}$. Taking into account that $Y_{J,y}$ is a union of the sets $(1 + J_p)y'$, we conclude that $|J_p|$ divides $|Y_{J,y}|$. By (62) this means that $|M|$ is coprime to p. Since the abelian group $R_p^\times$ acts transitively on M, this implies that $1 + \mathrm{rad}(R_p)$ is a subgroup of the kernel of this action. Therefore $(1 + \mathrm{rad}(R_p))Y = Y$, and hence

$$(1 + \mathrm{rad}(R_p))(1 + J)X = (1 + \mathrm{rad}(R_p))Y = Y = (1 + J)X.$$

In particular, given $u \in 1 + \mathrm{rad}(R_p)$ and $z \in X$ one can find $u' \in 1 + J$ and $z' \in X$ such that $uz = u'z'$. It follows that $(u/u')X = X$. When u runs over the elements of highest order in $1 + \mathrm{rad}(R_p)$, the element $(u/u')_p$ runs a full system of representatives of $(1 + J_p)$-cosets in $1 + \mathrm{rad}(R_p)$. Therefore the Sylow p-subgroup of the group K generated by all elements u/u' coincides with $1 + \mathrm{rad}(R_p)$. Since $KX = X$, the equality (61) holds and we are done.

References

[1] E. Bannai, T. Ito, *Algebraic combinatorics. I*, Benjamin/Cummings, Menlo Park, CA, 1984.

[2] J. D. Dixon, B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, No. 163, Springer-Verlag New York, 1996.

[3] S. Evdokimov, I. Ponomarenko, *On a family of Schur rings over a finite cyclic group*, Algebra and Analysis, **13** (2001), 3, 139–154. (English translation in St. Petersburg Math. J., **13** (2002), no. 3, 441–451.)

[4] S. Evdokimov, I. Ponomarenko, *Characterization of cyclotomic schemes and normal Schur rings over a cyclic group*, Algebra and Analysis, **14** (2002), 2, 11–55. (English translation in St. Petersburg Math. J., **14** (2003), no. 2, 189–221.)

[5] S. Evdokimov, I. Ponomarenko, *Recognizing and isomorphism testing circulant graphs in polynomial time*, Algebra and Analysis, **15** (2003), 6, 1–34. (English translation in St. Petersburg Math. J., **15** (2004), no. 6, 813–835.)

[6] S. Evdokimov, I. Ponomarenko, *A new look at the Burnside-Schur theorem*, Bulletin of the London Mathematical Society, **37** (2005), 535-546.

[7] S. Evdokimov, I. Ponomarenko, *Normal cyclotomic schemes over a finite commutative ring*, Algebra and Analysis, **19** (2007), 58–84. (English translation in St. Petersburg Math. J., **19** (2008), 911-929.)

[8] S. Evdokimov, I. Ponomarenko, *Schur rings over a Galois ring of odd characteristic*, Preprint POMI, (2008), 1–23, accepted to Journal of Combinatorial Theory, Ser. A (2009).

[9] S. Evdokimov, I. Ponomarenko, *Permutation group approach to association schemes*, European Journal of Combinatorics, **30** (2009), 6, 1456–1476.

[10] R. W. Goldbach, H. L. Claasen, *Cyclotomic schemes over finite rings*, Indag. Math. (N.S.), **3** (1992), 301–312.

[11] I. Kovács, *Classifying Arc-Transitive Circulants*, J. Algebraic Comb., **20** (2004), 353–358.

[12] K. H. Leung, S. H. Man, *On Schur Rings over Cyclic Groups, II*, J. Algebra, **183** (1996), 273–285.

[13] K. H. Leung, S. H. Man, *On Schur Rings over Cyclic Groups*, Israel J. Math., **106** (1998), 251–267.

[14] B. R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics, Vol. 28, Marcel Dekker Inc., New York, 1974.

[15] M. E. Muzychuk, *On the structure of basic sets of Schur rings over cyclic groups*, J. Algebra, **169** (1994), no. 2, 655–678.

[16] M. Muzychuk, *A solution of the isomorphism problem for circulant graphs*, Proc. London Math. Soc., **88** (2004), 1–41.

[17] H. Wielandt, *Finite permutation groups*, Academic press, New York - London, 1964.